UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

AMERICAN CIVIL LIBERTIES UNION, et al. Plaintiffs, v. ALBERTO R. GONZALES, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES Defendant.	Civil Action No. 98-CV-5591

PLAINTIFFS' PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW

I. STIPULATED FACTS

1. Defendant, Alberto R. Gonzales, is the Attorney General of the United States, who is charged with enforcing the provisions of the Child Online Protection Act ("COPA") challenged in this action.

2. Plaintiffs represent a range of individuals and entities including speakers, content providers, and ordinary users on the World Wide Web (the "Web"), as that term is defined in the Act. Plaintiffs post content including, *inter alia*, resources on sexual health, safe sex, and sexual education; visual art and poetry; resources for gays and lesbians; online magazines and articles; music; and books and information about books that are being offered for sale.

3. Some of the Plaintiffs provide interactive fora on their Web sites, such as online discussion groups, bulletin boards and chat rooms, which enable users to create their own material on Plaintiffs' Web sites. Some of the verbal and visual exchanges that

could potentially occur in these chatrooms or in the postings on their bulletin boards may include language or images that contain sexual content.

4. Plaintiff ACLU is a nationwide, non-partisan organization which states that it is dedicated to defending the principles of the Bill of Rights. ACLU members Patricia Nell Warren and Lawrence Ferlinghetti engage in speech on the Internet.

5. Plaintiff ACLU sues in part on behalf of its member Lawrence Ferlinghetti, who is a writer and San Francisco's poet laureate. Mr. Ferlinghetti is the co-founder of City Lights Bookstore, which maintains a Web site "that promotes books available from the bookstore" and "contains lists of literary events and a brief history of City Lights Bookstore and Publishing," has a section describing Mr. Ferlinghetti's 1956 obscenity trial for selling the Allen Ginsberg poem "Howl," and also has Mr. Ferlinghetti's poetry.

6. The City Lights Bookstore Web site states that "City Lights is a landmark independent bookstore and publisher that specializes in world literature, the arts, and progressive politics." The Web site also states that:

> For almost half a century, City Lights has demonstrated a commitment to preserving and promoting the diversity of voices and ideas that are represented in quality books. Now, as information technologies change the way people live and think, we are convinced that a community that continues to value writing and reading is essential to the future of a democratic society. With this in mind, we formed the City Lights Foundation, a non-profit cultural and educational foundation with the goal of advancing literacy and the literary arts.

7. Plaintiff ACLU also sues in part on behalf of Patricia Nell Warren, who is an author of novels, poetry, numerous articles, and essays. Her novels are alleged to be the most popular novels among classic gay literature. Ms. Warren is a co-owner of Wildcat International and its publishing arm, Wildcat Press. The Web site for Wildcat

Press contains excerpts of her work, including "sexually explicit details such as the description of a 'foursome' erotically dancing and a description of two men passionately kissing." The Wildcat International Web site states that "Wildcat International is an independent media company offering the real edge in writing, publishing, filmmaking, special events, and media consulting."

8. Plaintiff Condomania states that it is the nation's first condom store and a leading seller of condoms and distributor of safer sex materials. Condomania engages in speech on the Internet.

9. Plaintiff Heather Corinne Rearick is a writer, artist, sex-educator, and activist whose primary presence on the Web consists of Scarletletters.com, Scarleteen.com, and Femmerotic.com.

10. Plaintiff Heather Corinne Rearick alleges that she maintains three Web sites, "each of which deals with issues of sex and sexuality with an explicit focus on challenging and combating the sexual oppression of traditionally marginalized groups."

11. Ms. Rearick operates the Web site scarleteen.com. "Scarleteen is the Internet's largest independent, unaffiliated, free resource for young adult sex education, information, and discussion, serving nearly two million teens, young adults, parents, and educators each year." The Scarleteen Web site states that "[w]e offer Scarleteen as a far better resource for sex information for teens than adult sexuality sites, as well as a supplement to in-home and school-based sex education. Many parents we have heard from have used it as a tool to initiate discussion with their teens on some of the topics addressed. Homeschooling parents have used Scarleteen as curricula for sex education; colleges add our articles to their syllabi often."

12. "Femmerotic is Heather Corinne [Rearick]'s personal Web site for showcasing her photographic and textual work and providing an 'open and intimate look at her life as an artist and activist.'" On this Web site Ms. Rearick states that "[g]enerally, I intend to examine sexuality, to document sexual relationship, to explore the human body and how I and viewers perceive it, to examine the female body and feelings about it, to explore my own identity and use all those aims to create work that creates questions."

13. Plaintiff Electronic Frontier Foundation ("EFF") sues in part on behalf of John W. "Bill" Boushka, who has worked on the Web site www.doaskdotell.com. In the Amended Complaint, Mr. Boushka states that he fears prosecution for his book "Do Ask, Do Tell: A Gay Conservative Lashes Back," which he describes as "an exposé about gays in the military" that is a "politically-charged text" containing "subject-matter and language that might be deemed harmful to minors." Doaskdotell.com states that "[t]his site (with the sister site[] . . . billboushka.com) presents an objective approach (that I call 'Do Ask, Do Tell') to social and political issues ("sociology"), where arguments and counter-arguments are directly compared."

14. Another Web site Mr. Boushka mentions in the Amended Complaint, hppub.com, is now defunct.

15. Plaintiff Free Speech Media, in partnership with Public Communicators Inc., operates freespeech.org, which provides speech on the Internet.

16. Plaintiff Free Speech Media, LLC operates a Web site "designed to encourage the democratic expression of progressive ideals through promoting, curating and hosting independent creators of audio and video content on the Web." Its video and

audio files "cover a wide range of topics, including human rights, homelessness, labor issues, racism, prison conditions, sexuality, AIDS, feminism and environmentalism." The Free Speech TV Web site states that "[s]eizing the power of television to expand social consciousness, FSTV fuels the movement for progressive social, economic, and political transformation. By exposing the public to perspectives excluded from the corporate-owned media, FSTV empowers citizens to fight injustices, to revitalize democracy, and to build a more compassionate world." The Web sites also states that "Free Speech TV broadcasts independently-produced documentaries dealing with social, political, cultural, and environmental issues; commissions and produces original programming; develops programming partnerships and collaborations with social justice organizations; provides special live broadcasts from remote locations; and maintains an adjunct Web site that hosts one of the Internet's largest collection of progressive audio and video content."

17. Plaintiff Nerve.com, Inc. is an online magazine which states that it is devoted to sexual literature, art, and politics. Nerve.com is run by Rufus Griscom.

18. Plaintiff Aaron Peckham d/b/a Urban Dictionary operates an online dictionary of contemporary slang.

19. Plaintiff Aaron Peckham d/b/a Urban Dictionary operates "an online slang dictionary whose terms and definitions are solely user-generated and user-rated."

20. Plaintiff Philadelphia Gay News states that it has been the leading print newspaper for the gay and lesbian community in Philadelphia since 1976. It is now published on the Internet.

21. Plaintiff Philadelphia Gay News ("PGN") is the "oldest gay newspaper in Philadelphia" and publishes both in print and online. The online and print editions "share much of the same content, including national and local news stories written by PGN correspondents, arts and events sections, regular columns, a calendar of events, and editorials on a variety of social and political topics." The online edition also contains personal and classified advertisements.

22. Plaintiff American Booksellers Foundation For Free Expression (ABFFE) is a non-profit organization founded by the American Booksellers Association. Plaintiff Powell's Bookstore is a member of ABFFE.

23. Plaintiff Powell's Bookstore operates seven bookstores in Portland, Oregon. Powell's has a Web site.

24. Plaintiff Powell's Bookstores states that it is the "world's largest independent new and used bookstore" and operates a Web site that "allows users to browse and purchase new, used, rare, and out-of-print books."

25. Plaintiff Salon Media Group publishes an online magazine featuring articles on current events, the arts, politics, the media, and relationships.

26. Plaintiff Salon Media Group, Inc. ("Salon") states that it "is a well-known, popular on-line magazine" that contains "news articles; commentaries on and reviews of music, art, television, and film; and regular columns on politics, relationships, the media, business, and other areas of interest." Salon's "goal is to break news as well as produce the most compelling sort of social commentary . . . on the web," and it seeks to attract a "broad general interest audience" with its readership.

27. Plaintiff Sexual Health Network owns and operates sexualhealth.com, which is dedicated to providing easy access to sexuality information, education, and other sexuality resources. Sexual Health Network is owned and operated by Mitchell Tepper.

28. Plaintiff Sexual Health Network has a Web site "dedicated to providing easy access to sexuality information, education, support and other sexuality resources for everyone, including those with disability, chronic illness or other health-related problems." It is run by Dr. Mitchell Tepper, who has a doctorate in Human Sexuality Education and a master's degree in Public Health. The Sexual Health Network Web site provides information to minors, as well as adults.

29. Plaintiff Electronic Privacy Information Center ("EPIC") "is a nonprofit educational organization established in 1994 to examine civil liberties and privacy issues arising on the Internet." EPIC alleges that it accesses information on the Internet, including sexually explicit pages, as part of its mission, which includes reporting on how well content filters work.

30. All of the plaintiffs express a subjective fear of prosecution under the statute.

31. No Plaintiff has ever been contacted by state or local authorities, nor prosecuted nor arrested regarding any investigation into criminal violations.

32. Every Plaintiff has Web pages that are blocked by at least two filtering companies in categories designed to assist parents in protecting their children from inappropriate speech about sex.

33. Ms. Warren acknowledges the serious literary value of her works, as the Wildcat International Web site states: "Patricia Nell Warren's novels have become

essential gay literature for bookstores, libraries and college courses worldwide and, according to recent surveys of independent book sales, are the most popular novels among classic gay literature." Ms. Warren believes that adults and minors "should have the right to access speech provided on the Wildcat Web site."

34. The Scarleteen.com Web pages identified by Plaintiff Rearick as representative of those about which she fears prosecution include Web site's front page, the discussion group front page, and the "front pages, and 'Articles' and 'Advice' subsections" of the Web site sections entitled: Body, SexYOUality, Reproduction, Infection Section, Pink Slip, Boyfriend, Take Two, Gaydar, and Sexual Politics.

35. Scarlet Letters is a Web site containing works of an artistic nature. The Web site states, "Since February of 1998, Scarlet Letters has been one of the Web's premier publisher of humanist, feminist, sex positive original and visionary creative and artistic work of all kinds." Furthermore, the Web site states, "Our goal is to give our readers an international and unique perspective on artistic expression without pretension or arbitrary limits."

36. Ms. Rearick describes her work on the photography home page in this manner:

> Blending more traditional styles, archetypes and themes with new approaches, keeping the physical and emotional tone real, grounded, varied and intense, I try to step outside genre by creating work that explores sexuality, gender and personal identity within fine art without a typical fine art nude genericism or loss of personal identity of the subject.

37. Free Speech Media identified five videos as a representative sample upon which it fears prosecution. Free Speech also stated that it maintains a community page, which contains material and links that "contain or may contain in the future, among other things, candid and explicit comments or questions on a diverse category of topics posted

directly by internet Web users." Some of the videos identified by Free Speech Media in its Amended Complaint and in discovery are no longer available on the Web site.

38. Nerve has won multiple awards for both its prose and photography." Nerve was one of five finalists for the National Magazine Award for General Excellence Online in 2005, along with Atlantic Monthly, Consumer Reports, Business Weekly and Style.com.

39. Nerve states in a general manner that its Web site "includes many photographs of nude and semi-nude persons taken by professional photographers such as Nan Goldin, Bettina Rheims, and Sylvia Plachy, and by the site's own users."

40. In response to interrogatories, Nerve listed material in four sections about which it fears prosecution: the Web site's nominations for its "Henry Miller Award" in the fiction section; the free tour available within the photography section, the "Blog-A-Log" section, in which readers can read about the dating experience of Nerve contributors in personal blogs, and the blog section of the Web site.

41. Mr. Peckham's asserted fear of prosecution is based on the fact that "Urban Dictionary contains material that may be considered 'harmful to minors' in some communities," because "[d]ozens of the words, phrases, and definitions found on urbandictionary.com humorously, graphically, or symbolically describe human anatomy and sexual acts." In the Amended Complaint and in response to Interrogatories, Mr. Peckham listed slang terms for which he feared prosecution.

42. Urban Dictionary is designed for users to share definitions of a variety of slang words, including words of a sexual nature. Mr. Peckham asserts that "Letters to the

site from students, parents, lawyers, educators, reporters, media translators and lexicographers attest to the site's cultural significance."

43. Philadelphia Gay News ("PGN") fears prosecution because it deals with "issues relevant to the gay and lesbian community," that "some communities would consider access to personal advertisements inappropriate for minors when involving persons of the same gender," and that "some communities" may believe PGN's descriptions of social and sports clubs catering to the gay and lesbian community to be harmful to minors "because they 'entice' young people into exploring gay life."

44. PGN identified printouts of Web pages about which it fears prosecution. Many of the pages about which PGN alleged a fear of prosecution, such as the "Philly Encounters" section and advertisements therein, as well as chat rooms, are no longer on the Web site.

45. ABFFE explained the type of material that its members seek to access. ABFFE describes it as material that contains "nudity and sexual conduct," such as the books *Primary Colors* by Anonymous and *Sabbath's Theater* by Philip Roth.

46. EPIC fears that if COPA were to go into effect the Web sites it reviews "may remove from their Web sites material similar to that which EPIC staff heretofore have been able to access" without providing proof of age. EPIC alleges that COPA compromises the right to access speech anonymously and that it "does not intend to instruct its staff to use a credit card or adult access code" to access Web sites.

47. Existing laws make it illegal to distribute material over the Internet that constitutes obscenity, 18 U.S.C. ch. 71, or child pornography, 18 U.S.C. ch. 110. From 2000 to 2005, Defendant initiated fewer than 20 prosecutions for obscenity which did not

also accompany charges of child pornography, travel in interstate commerce to engage in sex with a minor, or attempting to transfer obscene material to a minor.

48. There have been fewer than 10 prosecutions for obscenity which did not also accompany charges of child pornography, travel in interstate commerce to engage in sex with a minor, or attempting to transfer obscene material to a minor since 2005.

49. Existing law prohibits the use of misleading domain names by Web sites. 18 U.S.C. § 2252B. Since the effective date of the statute in 2003, Defendant has initiated fewer than 10 prosecutions under the Misleading Domain Names statute.

50. The Internet is an interactive medium based on a decentralized network of computers.

51. On the World Wide Web, a client program called a Web browser retrieves information resources, such as Web pages and other computer files, from Web servers using their network addresses and displays them, typically on a computer monitor, using a markup language that determines the details of the display. One can then follow hyperlinks in each page to other resources on the World Wide Web of information whose location is provided by these hyperlinks. The act of following hyperlinks is frequently called "browsing" or "surfing" the Web.

52. Web pages are often arranged in collections of related material called "Web sites," which consist of one or more "Web pages."

53. To navigate to different pages on the Web, an HTTP request is sent to the Web server working at that IP address for the page required. In the case of a typical Web page, the HTML text, graphics and any other files that form a part of the page will be requested and returned to the client (the Web browser) in quick succession. The Web

browser's job is then to render the page as described by the HTML and other files received, incorporating the images, links and other resources as necessary. This produces the on-screen "page" that the viewer sees. Most Web pages contain hyperlinks to other relevant and informative pages and perhaps to downloads, source documents, definitions and other Web resources.

54. Some Web sites serve as a proxy or intermediary between a user and another Web page. When using a proxy server, a user does not access the page from its original URL, but rather from a URL on the proxy server.

55. Modern search engines search for and index Web pages individually. Search engines are Web sites that provide links to relevant Web pages, in response to search terms (words or phrases) entered by a user. They are a popular way of finding information online.

56. Most users interact with the Web by using a search engine. A search engine is a computer program designed to help find information stored on a computer system such as the World Wide Web. The search engine allows the user to request content that meets specific criteria (typically those containing a given word or phrase) and to retrieve a list of references that match those criteria.

57. Internet content filtering software attempts to block certain categories of material that a Web browser is capable of displaying, including "adult" material. Filters categorize Web sites or pages based on their content. By classifying a site or page, and refusing to display it on the user's computer screen, filters can be used to prevent children from seeing material that might be considered unsuitable. In addition, businesses often

use filters to prevent employees from accessing Internet resources that are either not work related or otherwise deemed inappropriate.

58. Some Internet content filters can be purchased on a CD or downloaded from the Internet and installed on a personal computer. Some filters are designed to be run on a server in a corporate, library, or school environment. Other filters are built into the services provided by Internet Service Providers.

59. Filters use different mechanisms to attempt to block access to material on the Internet. Some filters use "black lists" to filter out content. Black lists are lists of Web site addresses (URLs) or Internet Protocol (IP) addresses that a filtering company has determined point to content that contains the type of materials their filter is designed to block.

60. In list-based filtering (sometimes called database or static filtering), the software draws on a database of pre-classified URLs and/or IP addresses. When a user requests a Web page (by entering a URL or IP address into a Web browser, or by clicking on a link) the filtering software checks it against the database and responds in whichever way it has been configured to respond.

61. A filter that allows access only to Web sites that have been thoroughly checked and found to contain no content in a certain category is called a "white list."

62. Some filters also use "white lists" of content that should never be blocked. White lists are lists of URLs or IP addresses that the filtering company has determined do not point to any content their filter is designed to block. A very restrictive filter might block all URLs except those included on a white list.

63. In addition to their own black and white lists, some filtering products give parents or administrators the option of creating customized black or white lists.

64. In addition to relying on black lists and white lists, some filters also use "key words" or other "dynamic filtering" techniques to attempt to limit access to certain Web pages. Filtering companies may compile lists of words and phrases associated with content that should be blocked, even if the page has not previously been categorized. Some products just attempt to remove those words from the page, while others attempt to block the entire Web page that contains these words or phrases.

65. A filter that responds solely to the text making up the name of an image file (*e.g.*, blowjob03.jpg) is a text-based filter, not an image-based filter. Similarly, filters that respond solely to the text making up the names of audio files (*e.g.*, screamingorgasm.mp3) or video files (*e.g.*, blowjobs.jpeg) are text-based filters (not audio-based or video-based filters).

66. Browsing the World Wide Web is one way in which individuals can use the Internet. The Internet can be used to engage in activities such as sending and receiving emails, trading files, exchanging instant messages, chatting online, streaming audio and video, and making voice calls.

67. Some filtering programs can be used by parents to prevent their children from having any access to parts of the Internet other than the Web, and to certain Internet applications which parents do not want their children to have any access to, such as e-mail, chat, instant messaging, newsgroups, message boards, and peer-to-peer file sharing.

68. Some content from the Internet is now capable of being viewed on devices other than traditional personal computers. Examples include mobile devices such as

mobile phones, personal digital assistants ("PDAs") such as the Blackberry, portable audio/video players such as the iPod, and game consoles such as the XBox or PlayStation.

69. The U.S. Census Bureau's Current Population Survey's results show that in September 2001, approximately 54 percent of the U.S. population was using the Internet from any location. That figure rose to 59 percent in 2003.

70. According to Marv Johnson, legislative counsel for the ACLU, the creation of a "dot-xxx" top-level domain name is "not going to make a whole lot of difference" in stopping minors from finding pornography. (http://www.physorg.com/news12015.html)

71. Parents of minor children who borrow their parent's payment cards to make online purchases can ask their children what they are going to purchase.

72. The City Lights Bookstore Web site accepts payment cards on order pages for customers and on a donation page to the City Lights Bookstore foundation.

73. The Wildcat International Web site accepts payment cards on order pages for customers, retailers, and educational booksellers.

74. The Condomania Web site accepts payment cards on order pages for customers.

75. The Scarleteen Web site links users to PayPal, which accepts payment cards, for donations to help Scarleteen continue to provide comprehensive sex education. The Scarleteen Web site shop links users to second-party sellers that accept payment cards on order pages for users.

76. The Scarlet Letters Web site has a membership subscription page that links users with a second-party site that accepts payment cards. Membership is required for "access to all Scarlet's past issues and membership to Heather Corinne to boot, with nearly 4,000 original, high quality erotic photographs, fiction, poetry and nonfiction from the editor and founder of Scarlet Letters."

77. The Femmerotic Web site has a membership subscription page which takes users to a second-party site that accepts payment cards. Among other things, members obtain access to "[o]ver 5,000 of [Ms. Rearick's] high-quality, mindfully and independently produced fine art photographs . . . . Erotic and nonerotic portraiture, fine art nudes, gender and body image exploration, installation projects, drag, couples photography, and primarily intimate, personal self-portraiture."

78. The Free Speech Media Web site accepts payment cards at its online merchandise store. The Free Speech Media Web site also accepts payment cards for donations to help Free Speech Media.

79. The Urban Dictionary Web site's book section links users to Amazon.com, which accepts payment cards.

80. Salon restricts access to large portions of its Web site to viewers that either watch a video advertisement in order to get access for the day or to viewers that are subscribers. The Salon Web site has a membership subscription page that accepts payment cards. A Salon membership "support[s] independent journalism" and allows the user access to all Salon articles and the discussion forum. The online store on the Salon Web site links users to second-party sellers that accept payment cards.

81. The online store on the Sexual Health Network Web site links users to second-party sellers that accept payment cards.

82. FTP stands for file transfer protocol. It is used primarily to transfer files across the Internet.

83. HTTP stands for hypertext transfer protocol; it is widely used on the Internet.

84. Among the Web sites that use primarily HTTP are *The New York Times, Washington Post*, and even plaintiffs ACLU, Electronic Frontier Foundation, Electronic Privacy Information Center, and Salon Media Group.

85. Most URLs use HTTP.

86. The FBI, which is part of the Department of Justice, uses the Websense enterprise filter for its computers with access to the Internet. The FBI installed Websense to block content, such as advertisements on the Internet taking up large bandwith, and to protect the institution from malicious codes and waste, fraud, and abuse of the Internet. Among the content blocked is content falling in the categories of pornographic and illicit adult material. Overall, the FBI is satisfied with the effectiveness of Websense to block content, although there have been reports of overblocking. The FBI has not performed an audit on the effectiveness of the Websense enterprise product in blocking sexual material.

87. The Bureau of Alcohol, Tobacco and Firearms, which is now part of the Department of Justice, uses the SmartFilter enterprise filter for its computers with access to the Internet. The ATF installed SmartFilter to block content, including sexually explicit material. The ATF reports that the SmartFilter product has fulfilled the requirements of its business needs, although there have been reports of overblocking.

The ATF has not performed an audit on the effectiveness of the SmartFilter enterprise product in blocking sexual material.

88. The Federal Bureau of Prisons (BOP), which is part of the Department of Justice, uses the SurfControl enterprise filter for its computers with access to the Internet. The BOP installed SurfControl to assist it in enforcing its policy that access to the Internet on BOP computers by its employees be primarily for the purpose of performance of official duties and to protect from waste, fraud, and abuse of the Internet. In furtherance of these objectives, BOP utilizes many of the categories provided by SurfControl, including the category that seeks to block sexually explicit Web content. If a BOP employee requests that a Web site be unblocked by SurfControl, he or she must obtain approval of his or her supervisor and the sole reason for consideration of unblocking any Web site is that access to the Web site is required solely for performance of official duties. BOP has a policy of denying such requests for personal reasons. Overall, the BOP is satisfied with the effectiveness of Surfcontrol to block content, although there have been reports of overblocking.

89. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a credit card.

90. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a debit card, including a reloadable prepaid card.

91. COPA does not reach non-commercial speech, even on the World Wide Web. 47 U.S.C. §231(a)(1); (e)(2)(A).

92. Congress has required Internet service providers (ISPs) and online service providers to "notify [all new customers] that parental control protections (such as computer hardware, software or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors." 47 U.S.C. §230(d). Congress also passed legislation that mandates the use of filtering programs in public schools and libraries that receive funds under two popular federal programs.

II. PLAINTIFFS' PROPOSED FINDINGS OF FACT

A. Plaintiffs and Their Websites

1. Many of the Plaintiffs are committed to providing uncensored Web sites. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka, December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998).

2. The vast majority of information on Plaintiffs' Web sites, as on the Web in general, is provided to users for free. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka, December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998; P. Exh. 37-46, 57.)

3. Similarly, the vast majority of information on Plaintiffs' Web sites, as on the Web in general, can be accessed immediately without any requirement that users register, provide a password or log-in, or otherwise provide any personal, identifying information in order to access the material. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka, December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998; P. Exh. 37-46, 57.)

4. Plaintiffs are commercial speakers on the Web. The speech on Plaintiffs' Web sites is designed to assist in making a profit. Although many of the Plaintiffs believe that much of the information available on their Web sites has non-commercial value, all of the information meets the definition of "for commercial purposes" under the Act. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka, December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998; P. Exh. 37-46, 57.)

5. Plaintiffs, like the universe of commercial speakers on the Web, have a variety of business models. Some of the Plaintiffs receive income by selling advertising on their Web sites. Some of the Plaintiffs sell goods over their Web sites, ranging from

millions of books, to condoms and other sexual health devices, to books that they authored themselves. Some of the Plaintiffs use the Web simply as an advertising and marketing tool -- a means of promoting their commercial activities. Some of the Plaintiffs generate revenue by combining these or utilizing other business models. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka, December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998; P. Exh. 37-46, 57.)

6. Web sites, including Plaintiffs' Web sites, depend on attracting a high level of traffic to their sites to attract and retain advertisers and investors. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka, December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998.)

7. The best way to stimulate user traffic on a Web site is to offer some content for free to users. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.)

8. With respect to those Plaintiffs and others who sell goods on their Web sites, only a small percentage of Internet users who visit those Plaintiffs' sites for information actually make a purchase. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.)

9. Although all of Plaintiffs' speech is commercial within the meaning of the statute, Plaintiffs believe that all of their speech has value, especially for adults and older minors. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka, December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998.)

10. If the Act is not permanently enjoined, some of the Plaintiffs intend to self-censor; others intend to risk liability and prosecution under the Act; and others have not yet decided what they will do. At least one Plaintiff has decided that, because it would be contrary to its mission to self-censor, it will have to forego the financial benefits of its commercial activities and become a noncommercial site if the Act is not permanently enjoined. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrina Rearick; Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; Miriam Sontz, November 17, 1998; Christopher Finan, November 16, 1998; John William Boushka,

December 8, 1998; John E. Noring, December 9, 1998; Marc Rotenberg, November 23, 1998; Marc Segal, December 9, 1998.)

11. Plaintiff EFF is a nationwide nonprofit organization that is committed to defending civil liberties in the world of online computer communication. EFF members access speech on the Internet. (Declarations of John William Boushka, December 8, 1998; John E. Noring, December 9, 1998.)

12. Plaintiff EPIC is a non-profit research organization that collects and distributes information concerning civil liberties and privacy issues arising in the new communications media. EPIC contributors access speech on the Internet. (Declaration of Mark Rotenberg, November 23, 1998.)

13. Plaintiff Patricia Nell Warren is a member of the American Civil Liberties Union, a nationwide nonpartisan organization of over 400,000 members dedicated to defending the principles of liberty and equality in the Bill of Rights. (Am. Compl. Dec. 8, 2004.) Ms. Warren is the author of numerous novels and other works, as well as the co-founder of Wildcat Press, which maintains a Web site that includes text and graphics. (Declaration of Patricia Nell Warren, Nov. 14, 1998.)

14. Plaintiff Lawrence Ferlinghetti is a member of the American Civil Liberties Union, a nationwide nonpartisan organization of over 400,000 members dedicated to defending the principles of liberty and equality in the Bill of Rights. (Am. Compl. Dec. 8, 2004.) Mr. Ferlinghetti is the author of numerous novels and other works, as well as the co-founder of City Lights Bookstore and Publishing. City Lights maintains a Web site that features an extensive selection of books, in topics ranging from

poetry and fiction to politics and music. (Declaration of Lawrence Ferlinghetti, Dec. 8, 1998.)

15. Plaintiff Powell's Bookstore is a reader-centered company that operates seven bookstores in Portland, Oregon, and maintains a Web site through which users can purchase new, used, rare, and out-of-print books. (Am. Compl. Dec. 8, 2004.) Powell's Bookstore is a longstanding member of the American Booksellers Foundation for Free Expression. (Declaration of Miriam Sontz, Sept. 15, 2006.)

16. Plaintiff American Booksellers for Free Expression ("ABFFE") is a non-profit organization created to inform and educate booksellers, other members of the book industry, and the public about the dangers of censorship. ABFFE promotes and protects the free expression of ideas. (Am. Compl. Dec. 8, 2004.)

Plaintiff Free Speech Media, LLC, in partnership with Public Communicators, Inc., is a non-profit organization that operates freespeech.org. This Web site promotes independent audio and video content on the Web.

17. Plaintiff Philadelphia Gay News is a for-profit corporation that has been the leading print and newspaper for the gay and lesbian community of Philadelphia since 1976. Philadelphia Gay News is also now published on the Web. (Am. Compl. Dec. 8, 2004.)

B. Plaintiffs and Other Speakers Reasonably Fear Prosecution As A Result of COPA.

18. Defendant's definition of speech covered by COPA has been inconsistent and unclear. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of

Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

19. Speech similar to that of Plaintiffs has been the subject of extensive efforts at censorship and prosecution around the country in recent years. In most cases, those efforts have been based on the importance of protecting children from speech about sex that adults consider harmful, patently offensive, and without value. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve, Henry Reichman, Wes Miller; P. Exh. 21-23, 47, 48.)

20. There are numerous examples of material on Plaintiffs' Web sites that contains nudity, sexual imagery, depictions or descriptions of sexual conduct or sexual acts, frank discussion of sexual topics, or explicit adult language or other matter that might be considered harmful to minors. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick; P. Exh. 37-46, 57, 118.)

21. Members of the ACLU have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Members of the ACLU similarly access speech on the Web that describes and depicts sexual acts and

sexual contact that is frank and explicit. Although those members believe their speech has value, even for older minors, they reasonably believe that many others do not share that view. (Declarations of Patricia Nell Warren, November 16, 1998; Lawrence Ferlinghetti, December 8, 1998; P. Exh. 43.)

22. Members of ABFFE have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although those members believe their speech has value, even for older minors, they reasonably believe that many others do not share that view. (Declaration of Christopher Finan, November 16, 1998; P. Exh. 46.)

23. Condomania contains speech that depicts and describes human genitalia, sexual acts, and sexual contact that is frank and explicit. Although Condomania believes its speech has value, even for older minors, Condomania reasonably believes that many others do not share that view. (Testimony of Adam Glickman, Henry Reichman; P. Exh. Exh. 40.)

24. Adam Glickman is aware of other Web sites that contain similar speech about human genitalia, sexual contact and sexual activity that is frank and explicit. (Testimony of Adam Glickman.)

25. Members of EFF have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although those members believe their speech has value, even for older minors, they reasonably believe that many others do not share that view. (Declarations of John William Boushka, December 8, 1998; John E. Noring; P. Exh. 118.)

26. EPIC employees and contributors distribute material over the Web that contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although these employees and contributors believe their speech has value, even for older minors, they reasonably believe that many others do not share that view. (Declaration of Marc Rotenberg, November 23, 1998.)

27. Free Speech Media contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although it believes its speech has value, even for older minors, Free Speech Media reasonably believes that many others do not share that view. (P. Exh. 44; Declaration of John Schwartz, September 14, 2006.)

28. Nerve.com contains speech that depicts and describes sexual acts and sexual contact that is frank and explicit. Although Nerve.com believes that its speech has value, even for older minors, Nerve.com reasonably believes that many others do not share that view. (Testimony of Rufus Griscom, Henry Reichman; P. Exh. 21-23, P. Exh. 38.)

29. Rufus Griscom is aware of other Web sites that contain similar speech about sexual contact and sexual activity that is frank and explicit. (Testimony of Rufus Griscom.)

30. Philadelphia Gay News contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although it believes its speech has value, even for older minors, Philadelphia Gay News reasonably believes that many others do not share that view. (Declaration of Mark Segal, December 9, 1998; P. Exh 45.)

31. Powell's Bookstores contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although it believes its speech has value, even for older minors, Powell's Bookstores reasonably believes that many others do not share that view. (Declaration of Miriam Sontz; P. Exh 46.)

32. Sexual Health Network contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although Sexual Health Network believes its speech has value, even for older minors, Sexual Health Network reasonably believes that many others do not share that view. (Testimony of Mitchell Tepper, Henry Reichman; P. Exh. 21-23, P. Exh. 37.)

33. Mitch Tepper is aware of other Web sites that contain similar speech about sexual acts and sexual contact that are frank and explicit. (Testimony of Mitchell Tepper.)

34. Salon.com contains speech that describes sexual acts and sexual contact that is frank and explicit. Although Salon believes its speech has value, even for older minors, Salon reasonably believes that many others do not share that view. (Testimony of Joan Walsh, Henry Reichman; P. Exh. 21-23, P. Exh. 39.)

35. Joan Walsh is aware of other Web sites that contain similar speech about sexual contact and sexual activity that are frank and explicit. (Testimony of Joan Walsh.)

36. UrbanDictionary.com contains speech that describes sexual acts and sexual contact that is frank and explicit. Although UrbanDictionary.com believes its speech has value, even for older minors, UrbanDictionary.com reasonably believes that many others do not share that view. (Testimony of Aaron Peckham, Henry Reichman; P. Exh. 21-23; P. Exh. 41.)

37. Aaron Peckham is aware of other Web sites that contain similar speech about sexual contact and sexual activity that are frank and explicit. (Testimony of Aaron Peckham.)

38. Heather Corrina Rearick operates three Web sites that contain speech that depict and describe human genitalia or the post-pubescent female breast, sexual acts, and sexual contact that is frank and explicit. Although Ms. Rearick believes that the speech has value, even, in most instances, for older minors, Ms. Rearick reasonably believes that many others do not share that view. (Testimony of Heather Corrine Rearick, Henry Reichman; P. Exh. 21-23, P. Exh. 42.)

39. Ms. Rearick is aware of other Web sites that contain similar speech about sexual contact and sexual activity that are frank and explicit. (Testimony of Heather Corrine Rearick.)

40. Wesley Miller engaged in speech on the outside wall of his art gallery in Pilot Point, Texas that included an image of Eve depicting her post-pubescent female breast. Mr. Miller was threatened with prosecution by the police under a statute prohibiting speech that is harmful to minors. (Testimony of Wesley Miller; P. Exh. 47-48.)

41. Wayne Snellen is an artist and is Director of the Leslie/Lohman Gay Art Gallery. Mr. Snellen's own art contains speech that depicts human genitalia, sexual acts, and sexual contact, including by same-sex couples, that is frank and explicit. The Gallery contains the work of many other artists whose art is similar and also includes depictions of the post-pubescent female breast. The art is available on the Web. Although

Mr. Snellen believes the speech has value, even for older minors, he reasonably believes that many others do not share that view. (Testimony of Wayne Snellen; P. Exh. 49.)

42. Mr. Snellen is aware of other Web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit. (Testimony of Wayne Snellen.)

43. Ms. Alicia Smith is a hip-hop musician who performs under the name God-Des. Her lyrics contain speech that describes human genitalia, post-pubescent female breasts, sexual acts, and sexual contact that is frank and explicit. Sound clips of her work are available on the Web. Although God-Des believes her speech has value, even for older minors, she reasonably believes that many others do not share that view. (Testimony of Alicia Smith; P. Exh. 50, 51, 83.)

44. Ms. Smith is aware of other Web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit. (Testimony of Alicia Smith.)

45. Ms. Marilyn Jaye Lewis is the founder and Director of the Erotic Authors Association (EAA), which operates a Web site. She is an author herself. Her work and work by other authors can be found on the Web site. The Web site contains speech that describes human genitalia, the post-pubescent female breast, sexual acts, and sexual contact that is frank and explicit. Although Ms. Lewis believes the speech has value, even for older minors, she reasonably believes that many others do not share that view. (Testimony of Marilyn Lewis; P. Exh. 12, 13, 52.)

46. Ms. Lewis is aware of other Web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit. (Testimony of Marilyn Lewis.)

47. Ms. Barbara DeGenevieve is a visual artist who works in drawings, photographs, articles, and film. Her Web site contains speech that depicts and describes human genitalia, the post-pubescent female breast, sexual acts, and sexual contact that is frank and explicit. Although she believes her speech has value, even for older minors, she reasonably believes that many others do not share that view. (Testimony of Barbara DeGenevieve; P. Exh. 53.)

48. Ms. DeGenevieve is aware of other Web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit. (Testimony of Barbara DeGenevieve.)

49. Ninety percent of Internet users have used search engines. When a user does a search, he is given a series of Web pages, not Web sites, to select. For that and other reasons, it is more accurate to think of a Web page "as a whole" than an entire Web site. (Testimony of Edward Felten.)

50. Other than the express words of the statute, Defendant has no policies, guidelines, criteria or rationales for determining whether certain material is "harmful to minors," as defined by COPA. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to

Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

51. Other than the express words of the statute, Defendant has no policies, guidelines, criteria or rationales for claiming that there is speech that is harmful to minors, but not obscene. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

52. Because Defendant has no policies, guidelines, criteria or rationales for determining whether certain material is harmful to minors, a Web site operator has no means of determining whether its Web site is covered by COPA other than by looking at the express words of the statute. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick; Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental

Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

53. According to Defendant, the only speech covered by COPA is that which is harmful to a 16-year-old. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5.)

54. Thus, the only speech that is covered by COPA but is not covered by existing obscenity statutes is speech which is harmful to a 17-year-old but not obscene. There is no such speech. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; 18 U.S.C. §71; Miller v. California, 413 U.S. 15 (1973).)

55. According to Defendant, all speech that is prurient for 16 year-olds is prurient for 17 year-olds. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5.)

56. According to Defendant, all speech that is patently offensive for 16 year-olds is patently offensive for 17 year-olds. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5.)

57. According to Defendant, all speech that lacks serious literary, artistic, political, or scientific value for 16 year-olds lacks serious literary, artistic, political, or scientific value for 17 year-olds. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5.)

58. According to Defendant, there is no speech that is harmful to a 16 year-old that is not also harmful to a 17 year-old. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental

Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5.)

59. According to Defendant, photographs of topless women exposing post-pubescent breasts can be harmful to minors in certain circumstances and not harmful to minors in other circumstances in some ill-defined contexts. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

60. Defendant has not and cannot identify any criteria or rationale for making the distinction that certain photographs of topless women exposing post-pubescent breasts are harmful to minors in certain circumstances and not harmful to minors in other circumstances. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental

Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

61. According to Defendant, a photograph of topless women exposing post-pubescent breasts on Playboy.com's Web site is not harmful to minors. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

62. According to Defendant, a photograph of topless women exposing post-pubescent breasts on Penthouse.com's Web site is harmful to minors. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated

March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

63. According to Defendant, a photograph of a topless woman exposing post-pubescent breasts, where the nipples are covered by superimposed "stars," is harmful to minors. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

C. COPA's Affirmative Defenses Do Not Cure Its Deficiencies.

(a) In General

64. There are no age verification services or products available to Web sites that actually verify the age of Internet users. There are no services or products that can effectively prevent access to Web sites by a minor. (Testimony of Michael Russo; P. Exh. 24, 25; Cadwell Dep. Tr. 46:19-48:3, 70:1-70:16; Meiser Dep. Tr. 29:25-30:5, 37:22-39:1, 40:3-41:12, 46:1-46:19, 71:23-72:11, 76:10-77:6, 77:21-78:2, 103:5-105:4, 121:14-122:19, 126:25, 128:2.)

65. There are fees associated with all verification services identified in COPA, as well as others that claim to provide age verification. Such fees apply any time a user attempts to access material on a Web site, even if there is no purchase. Such fees must either be paid by the Web site or passed on to the users. As a result, Web sites such as Plaintiffs', which desire to provide free distribution of their information, will be prevented from doing so. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick; P. Exh. 71, 72, 75, 77, 80, 105, 106; Thaler Dep. Tr. 104:20-105:5, 106:24-107:14, 108:2-108:19; Cadwell Dep. Tr. 89:4-90:18, 106:6-106:23, 117:11-117:16; Meiser Dep. Tr. 133:24-134:3, 137:2-137:21; Cadwell Dep. Exh. 9, Thaler Dep. Exh. 5, Meiser Dep. Exh. 3.)

66. There is no effective way for content providers or Web site operators, including Plaintiffs, to determine the identity or the age of a user who is accessing or providing material through Web-based interactive fora such as discussion groups or chat rooms. The only way to ensure that material does not reach minors in any such interactive forum is to place all messages in all interactive fora behind screens accessible only to those users whose ages have been verified. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick.)

67. Because of the nature of the Web, COPA would require that users of any interactive forum provide a credit or debit card or sufficient personal information to pass through an age verification screen before entering the discussion – even if the discussion contains a wide range of speech that is not harmful to minors. There is no method by which the creators of an interactive forum could block access only to material that is

"harmful to minors," but allow access to the remaining content, even if the overwhelming majority of that content is not harmful to minors. (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick.)

68. The majority of Web users already refuse to register or provide any real personal information to Web sites if they have any alternative. Because age verification is costly and difficult to use, and because requiring age verification would lead to a significant loss of users, many content providers will choose to self-censor rather than shoulder the larger burden of age verification. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.)

69. Because of the way search engines work, credit card or other COPA screens will prevent Web pages from being identified by search engines and, in turn, seen by users. Requiring use of age verification screens will have a negative effect on the operation of the Web. Search engines will, in particular, be affected by the widespread use of verification screens and the placement of material behind such screens. (Testimony of Edward Felten, Michael Russo; P. Exh. 1-2.)

70. Because COPA covers a broad range of material, each Web site would need to create some organizational policy for determining what is harmful to minors and what is not. To comply with COPA, a content provider would be required to apportion some of its staff, or to hire new staff members, to review old and new content. This content includes all images, text, sounds and videos. These individuals must be well-versed in the legal definition or the organization's policy and have the authority to decide

whether to place content into an "adult section." (Testimony of Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick.)

71. There are no adult access code products, within the meaning of 42 U.S.C. §231(c)(A), that verify age. (Testimony of Michael Russo; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories, dated Jan. 27, 2006.)

72. There are no digital certificates, within the meaning of 42 U.S.C. §231(c)(B), that verify age. (Testimony of Michael Russo; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories, dated Jan. 27, 2006.)

73. There are no other reasonable measures that are feasible under available technology, within the meaning of 42 U.S.C. §231(c)(B), that verify age. (Testimony of Michael Russo.)

74. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a debit card, including a non-reloadable prepaid card. 47 USC § 231 (c) (1).

75. Minors have access to credit cards. (Testimony of Michael Russo, Ronald J. Mann; P. Exh. 17, 25, 33, 34, 91, 92, 93, 97, 98; Bergman Dep. Ex. 2.)

76. Minors have access to debit cards. (Testimony of Michael Russo, Ronald J. Mann; P. Exh. 17, 25, 34, 91, 92, 93, 97, 98; Bergman Dep. Tr. 46:06-48:01; Bergman Dep. Ex. 2.)

77. Minors have access to reloadable prepaid cards. (Testimony of Michael Russo, Ronald J. Mann; P. Exh. 17, 25, 34, 91, 92, 93, 94, 95, 96, 97, 98, 99; Bergman Dep. Tr. 14:16-16:18, 48:02-50:05; Bergman Dep. Ex. 5.)

78. Minors have access to non-reloadable prepaid cards. (Testimony of Michael Russo, Ronald J. Mann; P. Exh. 17, 25, 34, 91, 92, 93, 97, 98; Bergman Dep. Tr. 14:16-16:18.)

79. There are millions of prepaid cards in circulation. (Bergman Dep. Tr. 62:17-63:05; Peirez Dep. Ex. 4.)

80. Web sites cannot choose to accept reloadable prepaid cards, but not accept non-reloadable prepaid cards. (Testimony of Michael Russo, D. Exh. D-439.)

(b) Deterrence

81. Because the vast majority of content on the Web is available for free, most Web users will not provide credit cards or personal information simply to obtain access to Web content. Requiring users to provide a credit card or personal information before they can browse a Web page to determine what it offers will deter most users from ever accessing those pages; Web sites such as Plaintiffs' will lose many users as a result. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.)

82. Requiring users to go through an age verification process would lead to a distinct loss in personal privacy. Many people wish to browse and access material privately and anonymously, whether viewing controversial or embarrassing content, reading about people they know, or considering purchases. Web users are especially not likely to provide a credit card or personal information to gain access to sensitive, personal, controversial or stigmatized content on the Web. As a result, many users who are not willing to access information non-anonymously will be deterred from accessing desired and necessary information, and Web sites such as Plaintiffs' will be deprived of

the ability to provide this information to such users. (Testimony Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.)

83. Although many users may risk transmitting their credit or debit card numbers over the Internet when they are making a purchase, many users are unlikely to take such a risk simply to access free content, particularly if that content is available on another Web site that does not require entry of that information. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.)

84. Widespread adoption of policies requiring users to provide a credit card or debit card, or to otherwise provide detailed personal information to pass through an age verification screen, would create additional identity theft risks for Web users and increase people's fears and security concerns about using the Internet. (Testimony of Michael Russo, Ronald J. Mann, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve; P. Exh. 34.)

85. Credit card companies advise consumers not to offer the card to merchants as a proxy for age. Bergman Dep. Ex. 3; Bergman Dep. Tr. 36:18-38:04.

86. COPA's requirement that Web sites maintain the confidentiality of information submitted for purposes of age verification would not alleviate the deterrent effect of age verification on users, because users must still disclose the personal information and then rely on third parties, many of whom are unknown and have no

actual person identified with them, to comply with the confidentiality requirement. The statute does not provide any recourse to users for confidentiality violations by Web sites. In fact, COPA explicitly grants immunity to content providers for any action taken to comply with COPA. 47 U.S.C. § 231(c)(2). (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.)

87. Requiring users to provide a credit card, debit card, adult access code, adult personal identification number or to otherwise go through an age verification screen before providing access to speech on the Web would completely bar many adults who lack such identification from access to information appropriate for them. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve.).

88. United States Web sites will suffer and be put at a distinct disadvantage because foreign Web sites will not have to comply with COPA. Most likely, the vast majority of non-U.S. Web sites will ignore COPA. As a result, many users, inside and outside the U.S., will gravitate toward non-U.S. sites that offer the same or similar information and services as U.S. Web sites, but that do not require the users to pass through an age verification screen. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve; Cadwell Dep. Exh. 10; Thaler Dep. Exh. 1.)

(c) Credit Card and Debit Card Verification

89. Credit card companies prohibit Web sites from claiming that use of a credit or debit card is an effective method of verifying age and prohibit Web sites from using credit or debit cards to verify age. (Testimony of Michael Russo; P. Exh. 26, 73, 74, 106; Bergman Dep. Tr. 36:18-38:04; 40:02-41:04; Bergman Dep. Ex. 4; Thaler Dep. Tr. 97:14-98:16, 98:17-99:13; Cadwell Dep. Tr. 95:18-96:9, 97:9-98:3.)

90. Many adults do not have credit or debit cards. (Testimony of Ronald J. Mann, Michael Russo; P. Exh. 34, 99.)

91. Many children have access to credit or debit cards. A significant percentage of minors have access to credit or debit cards with the express permission of their parents. A significant percentage of minors also have access to credit or debit cards without the knowledge or consent of their parents. The best estimate is that at least half of all children have such access. The percentage of 16 year-olds with access to payment cards is significantly higher than the percentage of 12 year-olds with access to payment cards. (Testimony of Ronald J. Mann; P. Exh. 17, 34, 90, 91, 93, 97, 98, 100; Bergman Dep. Tr. 14:16-16:18, 16:22-18:02, 18:03-18:07, 18:13-18:19, 18:25-19:03, 19:12-19:15, 19:16-20:25, 21:02-21:11, 34:06-35:21; Bergman Dep. Ex. 2; Rinchiuso Dep. Tr. 09:05-09:12, 09:13-09:18, 10:21-10:23; Peirez Dep. Tr. 09:06-09:21, 76:22-76:25.)

92. Many issuing agencies market credit and debit cards to minors. Payment card companies increasingly market cards directly to minors. Currently, one of the main thrusts of credit card marketing in this country is to get payment cards into the hands of youth as early as possible. This marketing focus is still rather new, and in the coming years, it is likely that this focus will result in more and more minors having payment cards. Visa's "Visa Buxx" card is one example of a payment card that is specifically

designed to be used by minors. (Testimony of Ronald J. Mann; P. Exh. 25, 34, 90, 98, 100; Bergman Dep. Tr. 14:16-16:18, 48:02-50:05 137:11-138:10; Bergman Dep. Ex. 3; Peirez Dep. Ex. 1, 2.)

93. Many employers, such as McDonalds, pay minor employees by providing them with payment cards. (Testimony of Ronald J. Mann.)

94. Payment card-based age verification schemes are not difficult to bypass. Minors can obtain payment card information to access "protected" areas of the Web through Web sites that offer those services. (Testimony of Michael Russo; P. Exh. 25, 81; Thaler Dep. Exh. 2, 10.)

95. There is no way for a merchant, such as a Web site, to know that a user is actually a minor. Merchants, including Web sites, that accept Visa or Mastercard credit cards or debit cards must honor all Visa or Mastercard credit cards or debit cards, including prepaid cards. (Testimony of Michael Russo, Ronald J. Mann; D. Exh. D-439; Bergman Dep. Tr. 16:22-17:22, 17:23-18:02; 48:02-50:05; Bergman Dep. Ex. 6; Peirez Dep. Ex. 3.; Thaler Dep. Tr. 57:19-58:15, 59:8-60:22; Cadwell Dep. Tr. 57:19-58:15, 59:8-60:22, 74:23-77:8.)

96. Financial institutions will not process or verify a payment card in the absence of a financial transaction. Express policies of the payment card companies prohibit online merchants who sell content from processing transactions in the amount of zero dollars ($0). Verification by payment card will therefore be practically infeasible for all of the Plaintiffs and most other Web site operators and content providers covered by COPA who distribute their content and material for free. (Testimony of Ronald J. Mann; P. Exh. 34; Rinchiuso Dep. Tr. 45:17-45:24; Thaler Dep. Tr. 121:25-122:6.)

97. The purpose of the payment card companies' processing systems is to process financial transactions or purchases. Those companies have regulations and policies designed to prevent their systems from being used for other, non-payment transaction-based purposes. Permitting zero-dollar transactions would threaten the system's capacity to process transactions, and would increase fraud by enabling criminals to enter numbers randomly into the system to identify active card numbers. (Testimony of Ronald J. Mann. P. Exh. 34.)

98. There is no reason for Web sites that do not sell anything – i.e., sites on which there is nothing for the user to purchase – to have relationships with any of the payment card companies. (Testimony of Michael Russo, Ronald J. Mann, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve; P. Exh. 34, 102, 103.)

99. Based on the payment card companies' past behavior and present policies, it is highly unlikely that they would enforce COPA against either domestic or overseas online content providers. The rare situations in which payment card companies have previously enforced laws against merchants involved inherently illegal transactions. These situations are not comparable to the enforcement of COPA. (Testimony of Ronald J. Mann; P. Exh. 101; Thaler Dep. Tr. 74:18 – 75:7; 79:15 – 80:2.)

100. Requiring use of a payment card to enter a site would impose a significant economic cost on Web entities. In addition to set-up fees and administrative fees, Web entities will also need to pay fees for processing payment card information. (Testimony

of Michael Russo; P. Exh. 72, 105, 106, 107; Thaler Dep. Tr. 107:3 – 107:14, 108:2 – 108:19, 109:12 – 110:14; Cadwell Dep. Tr. 89:4 – 90:18.)

101. In addition, if the cost is absorbed by the Web site, then people hostile to the Web site can access the Web site thousands of times in order to force the Web site to absorb the costs. (Testimony of Edward Felten, Henry Reichman).

102. There are fees associated with online purchases that are subsequently denied by the payment card holder (chargeback fees). Chargeback fees are higher for Web entities that provide content that is associated with a higher risk of a denial of payment. The risk of chargebacks is higher for Web entities that provide sexually explicit content that is controversial in the community. (Testimony of Michael Russo; Bergman Dep. Tr. 56:11-56:21, 76:06-77:03; Bergman Dep. Ex. 1, 7, 8, 9, 10; Thaler Dep. Ex. 1.)

103. Credit and verification charges must either be absorbed by the content provider or passed on to users. This cost will increase according to the number of visitors to a site. Many of the larger sites have well over a million unique visitors per day. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve; P. Exh. 72, 106.)

104. Credit cards are not commonly used for online transactions in Europe and Asia. The effect of COPA would be to divide the Web into two sections, one involving U.S. speakers who largely speak only to U.S. residents and another Web, composed of overseas sites who can speak to anyone including U.S. residents. (Testimony of Michael Russo.)

(c) Data Verification Services

105. A few companies offer non-payment card-based services and/or products that can be used in an attempt to verify age. These systems rely on a number of sources of public records, and some privately acquired information, in an attempt to verify age. Generally, these systems function by charging Web sites a per transaction fee in exchange for their checking personal data, supplied by the Web site's visitors, against a database of records either owned by or otherwise available to these systems. Before being given access to a Web site, a user will be required to provide specified personal information such as the person's name, last four digits of the social security number, home address, home telephone number, or driver's license number, on a Web form that is sent by the Web site to the verification system. The system will then check the data sent by the Web site against a database to see if the data matches that of an adult or a minor, or if the data cannot be verified, and then send the response to the Web site. Because these services essentially are checking data sources, rather than verifying the actual age of an individual, these services are more appropriately referred to as "data verification systems," rather than "age verification systems." (Testimony of Michael Russo; P. Exh. 25, 76, 77, 79, 104.)

106. These services are more likely to successfully match data provided by a Web site visitor to data contained in a database if more information, and especially more personal information, is provided. If the last four numbers of a social security number are provided, there is a much greater chance that a Data Verification Service will be able to match the information to one particular individual than if basic information such as a name, street address, and ZIP code are required. If the latter is all that is requested, there is a much greater chance that the system will not be able to match the provided data to

one particular individual and therefore whether it belongs to an adult or a minor. (Testimony of Michael Russo; P. Exh. 25, 76, 77, 78, 79.)

107. The Web site operator decides what information to request from a visitor. (Testimony of Michael Russo, P. Exh. 25, 76, 77, 80.)

108. The more information provided, the higher the fee charged by the DVS will be. The fee charged to Web site operators can range from approximately 25 cents to approximately one dollar per verification. There may also be other fees associated with using a DVS on top of the per transaction fees, such as setup fees. (Testimony of Michael Russo; P. Exh. 25, 75, 80; Meiser Dep. Tr. 133:24-134:3, 137:2-137:21, 176:4-176:15.)

109. DVS operators will return one of three general answers: data verified belongs does not belong to an adult; data verified belongs to an adult; data could not be verified. Others will assign a confidence level indicating the success rate in matching the provided data to public records. Upon receiving these responses, Website operators will need to determine whether or not they will grant access to the online content. (Testimony of Michael Russo; P. Exh. 25, 76, 77, 78,)

110. When COPA was first passed in 1998 and when this Court entered a preliminary injunction against enforcement of COPA in 1999, there were no data verification systems that accurately verified age. There are still no data verification systems that accurately verify age. (Testimony of Michael Russo; P. Exh. 25)

111. No data verification systems are able to verify accurately the age of everyone living in the United States. As a result, even adults living in the United States who submit valid and legitimate personal information to a DVS in order to access a Web

site can be denied access. (Testimony of Michael Russo; P. Exh. 25, 76, 77, 78, 79; Meiser Dep. Tr. 77:21-78:2.)

112. Existing data verification systems have an especially difficult time verifying data of individuals who are between 17 and 21 years old. Because many individuals in the United States who are over 16 years old cannot have their personal data verified by the existing data verification products, if Web sites such as Plaintiffs' utilize data verification products to comply with COPA, many adults will not be able to access those Web sites. (Testimony of Michael Russo; P. Exh. 79; Meiser Dep. Tr. 121:14-122:19.)

113. No data verification systems are able to accurately verify data of anyone who lives outside of the United States unless those individuals have U.S. public records. Because many individuals living outside the United States who are over 16 years-old cannot have their personal data verified by the existing data verification products, if Web sites such as Plaintiffs' utilize data verification products to comply with COPA, non-American adults will not be able to access those Web sites -- and the audience for those Web sites will be limited solely to Americans whose data could be verified -- even though there may be many people who might otherwise want to access the speech or content on the Web sites. (Testimony of Michael Russo; P. Exh. 25, 77, 79; Meiser Dep. Tr. 124:11-125:11.)

114. Because they often rely on basic personal information, such as a person's name and address, data verification systems are prone to abuse and can be circumvented with minimal effort by anyone, including minors, desiring to gain access to Web sites relying on data verification systems to verify age. That is, in part, because there is no

way for a data verification system (or a Web site utilizing such a system) to verify that the person entering the personal information is actually the person to whom that information pertains. Nor is there any way for the person to whom that information does pertain to know that his or her information has been used because the DVS companies do not notify people when their information has been run through a check. (Testimony of Michael Russo; Meiser Dep. Tr. 46:1-46:19, 103:5-105:4, 126:25-128:2, 128:17-128:20.)

(d) Digital Certificates

115. There are no digital certificates that can be used to comply with COPA. (Testimony of Michael Russo; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories, dated Jan. 27, 2006.)

(e) Other Reasonable Alternatives

116. No other available or feasible options exist that allow Web sites to restrict access to certain material by minors while continuing to provide it to adults. (47 U.S.C. § 231(c)(1(C); Testimony of Michael Russo; P. Exh. 25; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories, dated Jan. 27, 2006.)

D. COPA Is Under-Inclusive.

117. COPA's restrictions do not apply to email, chat, instant messaging, peer-to-peer file distribution networks, streaming video and audio content, Internet newsgroups, voice-over-Internet telephone calls, or Internet television. COPA also does not cover speech utilizing the ftp protocol. (Testimony of Edward Felten; P. Exh. 103.)

118. There is a significant amount of speech, including sexually explicit speech, that can be accessed using all of the forms of Internet speech listed in the prior paragraph. These modes of communication are used to distribute text, pictures, images, video, and audio content, among other things. (Testimony of Edward Felten, Rufus

Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve, Michael Russo; P. Exh. 14-17, 25, 27, 108, 109, 111-117, 119.)

119. Millions of people, including a significant number of minors, use these forms of Internet speech on a regular basis. For example, approximately 90 percent of all Internet users send or receive email. 75 percent of online teens send instant messages, and it is estimated that about 50 percent do so on a daily basis. Hundreds of millions of files are distributed over peer-to-peer networks each week, and it is estimated that about 30 percent of all people downloading video and music files do so via peer-to-peer technology. (Testimony of Edward Felten; P. Exh. 14-17.)

120. There is a significant amount of sexually explicit speech that can be accessed on the World Wide Web that is posted by sites that are not commercial. (Testimony of Michael Russo, Rufus Griscom, Joan Walsh, Adam Glickman, Mitchell Tepper, Aaron Peckham, Heather Corrine Rearick, Alicia Smith, Wayne Snellen, Marilyn Jaye Lewis, Barbara DeGenevieve; P. Exh. 25.)

121. There is a significant amount of sexually explicit speech on Web sites on the World Wide Web that is hosted or registered overseas. A conservative estimate places 32 percent of adult membership sites and 58 percent of free adult Web sites outside the United States. (Testimony of Michael Russo, Matthew Zook; P. Exh. 25, 28-29, 30-32, 55, 56.)

122. Adult Web sites are migrating out of the United States, and free adult Web sites are migrating at the highest rates. From 2001 to 2006, the United States' share of free adult Web sites dropped from 60 percent to 42 percent. This is occurring due to U.S.

regulations, low barriers to entry into the Internet adult entertainment business, and diffusion of Internet use. (Testimony of Matthew Zook. P. Exh. 30-32.)

123. Much commercial pornography on the Web, especially adult videos and the higher quality images, is only available to those who pay for it. (Testimony of Michael Russo; P. Exh. 25.)

124. Because U.S. adult Web sites that charge for viewing their content already require use of a payment card for users to get access to their material, those Web sites will not be affected by COPA due to the statute's credit card affirmative defense. Because minors have access to payments cards, the sexually explicit material on these Web sites will be available to minors even if COPA were to go into effect. (Testimony of Michael Russo; P. Exh. 25.)

125. Individuals wishing to evade COPA can do so by utilizing FTP instead of HTTP. The major browsers available today are capable of downloading files using the FTP protocol. For many file transfer or distribution applications, FTP is a viable alternative to HTTP. It is easy to use FTP instead of HTTP, and the necessary software is available for free. (Testimony of Edward Felten; P. Exh. 18-19.)

126. Speech that is communicated over email is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten.)

127. Speech that is communicated over peer-to-peer networks is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten; P. Exh. 119.)

128. Speech that is communicated via chat is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten; P. Exh. 119.)

129. Speech that is communicated via instant messaging is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten; P. Exh. 119.)

130. Speech that is communicated via streaming video and audio is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten; P. Exh. 119.)

131. Speech that is communicated via online television is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten.)

132. Speech that is communicated via newsgroups, such as USENET, is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten.)

133. Speech that is communicated via voice-over-Internet telephone calls is not covered by COPA and cannot be prosecuted under COPA. (Testimony of Edward Felten.)

134. All of the forms of Internet communications listed in the prior nine paragraphs can be used to communicate images as well as text. (Testimony of Edward Felten; P. Exh. 111-117, 119)

135. All of the forms of Internet communications listed in the prior nine paragraphs prior to the previous paragraph can be blocked, in whole or selectively, by Internet content filters. (Testimony of Edward Felten, Lorrie Cranor.)

E. There Are A Number of Less Restrictive Alternatives That Are At Least As Effective As COPA.

(a) Internet Content Filters

(i) Summary of Internet Content Filters

136. Internet service providers ("ISPs") and commercial online services like America Online provide parents with a wide range of mechanisms that parents can use to prevent their children from accessing material online that they do not want their children to view. Parents can tailor these services to their own values and to the age and maturity of their child. These services reach, and block, speech that is posted overseas, posted on non-commercial sites, or available in non-Web-based mediums, such as email, instant messaging, chat, newsgroups, peer-to-peer file sharing, and any other formats other than http. They can also be used to block all speech in all interactive fora. (Testimony of Lorrie Cranor; P. Exh. 86; Whittle Dep. Tr. 7:9-8:4; 15:2-16:17; 16:18-24:22; 25:1-25:1; 25:13-29:6; 30:14-31:5; 43:3-43:13; 48:9-49:11.)

137. Similar services and software are offered by numerous private software companies. (Testimony of Lorrie Cranor; Allan Dep. 68:7-70:13.)

138. Parents and other online users can use filtering programs, also known as user-based blocking programs, to restrict access to sexually explicit content. These programs allow users, among other things, to block access to sexually explicit Web pages, to prevent children from giving personal information to strangers by e-mail or in chat rooms, and to keep a log of all online activity that occurs on the home computer. (Testimony of Lorrie Cranor; Whittle Dep. 25:13-29:6.)

139. Internet content filters are computer programs designed to restrict access to certain types of material on the Internet. They are used frequently by employers to

restrict the Internet access of their employees, and by schools, libraries, and parents to restrict the Internet access of children. (Testimony of Lorrie Cranor, Terri Kirk, Clover Taylor, Tava Smathers.; Murphy Dep. 29:25-32:4)

140. Internet content filters can be programmed or configured in a variety of different ways. They can be set up to restrict materials based on the type of content they contain (adult material, information about drugs, etc.), the presence of particular words, the address of the Web site, or the Internet protocol or application used (World Wide Web, email, instant message, peer-to-peer, etc.). Some filters can also restrict access based on time of day, day of week, how long the computer has been connected to the Internet, or which user is logged onto a computer. (Testimony of Lorrie Cranor; P. Exh. 86; Allan Dep. Tr. 65:24-66:16; 68:7-70:13; 140:18-140:25; 141:1-142:25; Whittle Dep. Tr. 7:9-8:4; 11:1-11:15; 16:18-24:22; 25:1-25:1; 25:13-29:6; 30:14-31:5; 48:9-49:11.)

141. Some filtering programs offer only a small number of settings, while others are highly customizable, allowing a parent or other administrator to make detailed decisions about what to allow and what to block. (Testimony of Lorrie Cranor; P. Exh. 86; Allan Dep. Tr. 65:24-66:16; 68:7-70:13; 145:12-147:22; Whittle Dep. Tr. 7:9-8:4; 16:18-24:22; 25:1-25:1; 48:9-49:11.)

142. Some Internet content filters are built into the services provided by ISPs; a family that subscribes to an ISP that provides filtering services can usually take advantage of these services without installing additional software on their computer. Filters may also be built into cable modems, wireless access points, and other Internet access devices. Filters will also soon be available as part of Microsoft's new operating system, meaning that all computers that come with Microsoft's operating system installed

will have built-in parental control features. (Testimony of Lorrie Cranor; P. Exh. 86, 89 Allan Dep. Tr. 148:22-150:11; 154:16-155:22; Murphy Dep. Tr. at 69:5-70:18.)

(ii) Methodology of Internet Content Filters

143. Filters enable parents and others to control access to the Internet through a variety of different mechanisms. (Testimony of Lorrie Cranor; P. Exh. 5, 84, 86; Allan Dep. Tr. 68:7-70:13; Whittle Dep. Tr. 7:9-8:4; 16:18-24:22; 25:1-25:1; 25:13-29:6; 48:9-49:11.)

144. Some filters use "black lists" to filter out content. Black lists are lists of Web site addresses (URLs) or Internet Protocol (IP) addresses that a filtering company has determined point to content that contains the type of materials their filter is designed to block. Some companies offer black lists that are very extensive, containing millions of Web sites, many of which are published in languages other than English. (Testimony of Lorrie Cranor; Allan Dep. Tr. 15:19-16:16; Whittle Dep. Tr. 7:9-8:4; 15:2-16:17; 16:18-24:22; 25:1-25:1; Murphy Dep. Tr. at 28:24-29:4, 41:16-44:8, Murphy Dep. Ex. 8.)

145. Black lists may be compiled in a variety of ways. A filtering company may use an automated Web crawler to identify new URLs that may contain content that should be blocked. They may have human employees search for additional sites. They may also run frequent search engine queries using search terms likely to result in content that should be blocked in order to identify new Web sites containing such content. Filtering companies do this because a significant proportion of people find Internet content today through search engines, and mimicking these searches allows the companies to identify the sites that people are most likely to see and access. In addition, some companies review industry lists of popular Web sites, or "most viewed" Web sites, to ensure that their products cover those sites that Internet users are most likely to attempt

to access. They may also collect reports of URLs that should or should not be blocked from their users, from their business partners, or from governmental entities. Finally, filtering companies may purchase or otherwise acquire lists of Web sites from other entities, including search engines, to supplement the sites they have independently located. (Testimony of Lorrie Cranor; Allan Dep. Tr. 12:24-14:19; 15:19-16:16; 138:10-139:11; 203:20-204:9; Murphy Dep. Tr. at 17:4-17:18, 23:17-28:6, 29:25-32:4, 30:19-31:8, 35:3-35:15, 38:3-38:14, Murphy Dep. Ex. 1.)

146. Once the URLs are identified, filtering companies may use an automated system to evaluate the URLs and to decide which should be put on the black list, or they may have their employees check those URLs to confirm that they meet the blocking criteria. Some companies require human review of every site included on their content lists to ensure accuracy. When filtering companies identify URLs that meet their blocking criteria, they may set up their black lists to block just one particular Web page, a section of a Web site, or the entire Web site. (Testimony of Lorrie Cranor; Allan Dep. Tr. 20:23-22:3; 203:20-204:9; Murphy Dep. Tr. at 20:24-21:23, 23:17-28:6, 28:24-29:6, Murphy Dep. Ex. 1, A.)

147. Most filtering products that use black lists contain mechanisms for frequently updating these lists and providing those updates to their users. Many of these updates are done automatically, without requiring the user to do anything. (Testimony of Lorrie Cranor; Allan Dep. Tr. 203:20-204:9.)

148. In addition to their own black and white lists, many filtering products give parents or administrators the option of creating customized black or white lists. For example, AOL allows parents to specify URLs that they want to be blocked or allowed,

regardless of the default settings for a particular age category. Many filters allow these customized lists to be created for multiple users, on a user-by-user basis, enabling a parent who has a child who is 16 years old and a child who is 6 years old to create separate customized black lists and white lists for each child. In addition, if parents believe their child is mature enough to see some, but not all, sites of a particular type, they can set their filter accordingly. (Testimony of Lorrie Cranor; P. Exh. 86; Allan Dep. Tr. 68:7-70:13; 145:12-147:22; Whittle Dep. Tr. 7:9-8:4; 16:18-24:22; 25:1-25:1.)

149. Several of the filtering products have divided up their lists into multiple categories; parents can decide if they want to block or allow Web sites within each such category. These categories cover far more than just sexually explicit material, enabling parents to restrict their children's access to whatever kinds of content they choose, not just sexually explicit materials. For example, in addition to "adult" content, many of the filters have categories for drugs, weapons, violence, hate speech, and other subjects which some parents might find inappropriate for their children. Some companies that offer multiple content categories allow parents to place a particular site within whichever category they choose, even if this is not the default setting, enabling parents to change decisions made by the filtering company if the parent disagrees with the company's categorization. (Testimony of Lorrie Cranor; P. Exh. 7, 86; Allan Dep. Tr. 68:7-70:13; 145:12-147:22; Whittle Dep. Tr. 7:9-8:4; 16:18-24:22; 25:1-25:1; Murphy Dep. Tr. at 41:16-44:8, 64:8-69:4.)

150. In addition to relying on black lists and white lists, some filters also use "key words" or other real-time, dynamic filtering techniques to limit access to certain Web pages. Filtering companies may compile lists of words and phrases associated with

content that should be blocked, even if the page has not previously been categorized. Some products just remove those words from the page, while others block the entire Web page that contains these words or phrases. They may also develop templates that provide additional context and prevent over blocking – for example, that block the word "breast" when used in combination with the word "sexy," but not when used in combination with the words "chicken" or "cancer." (Testimony of Lorrie Cranor; Allan Dep. Tr. 92:19-93:15; 98:8-101:15; 112:23-113:21; Whittle Dep. Tr. 11:1-11:15; 16:18-24:22; 25:1-25:1; Murphy Dep. Tr. at 112:22-113:25.)

151. Some filters also use artificial intelligence or machine-learning techniques to teach their software to determine whether content should be blocked if it is not already on a list. Every time the software encounters a new Web page, the filter can analyze the content and determine how similar it is to the examples it has seen in the past and therefore whether or not it should be blocked. Much like other similar software, filtering products use statistical pattern recognition techniques to identify features of acceptable and unacceptable Web pages, which may include combinations of words, links, formatting, or other features. (Testimony of Lorrie Cranor; Allan Dep. Tr. 52:7-54:20; 63:8-65:1.)

152. Some filters apply these types of real-time techniques to image blocking, just as they do to text blocking. Filtering companies can use artificial intelligence or machine-learning techniques to "teach" their filters which images should be blocked. They can also use computer vision techniques to identify body parts or other visual images that should be blocked. Although image-filtering techniques by themselves tend to be less accurate than text filtering techniques, image filtering can be effective when

used in combination with text filtering techniques – for example, examining both images and the textual image captions to determine whether content should be blocked. Indeed, studies done by one of the filtering companies in connection with their mobile filtering product indicate that their image filter is 87 percent accurate if there is no text whatsoever on a page, and when the image filter is combined with their text-based product, the filter is 99.48 percent accurate. (Testimony of Lorrie Cranor; Allan Dep. Tr. 81:18-87:2; 89:10-89:17; 92:19-93:15; 98:8-101:15; 109:9-109:13; 174:7-178:15; Murphy Dep. Tr. at 60:19-64:7.)

153. The metadata, or hidden text tags, attached to Web sites also help filters to find and block inappropriate images. For example, if there is an image on a page, but no visible text or caption, and the metadata identifies it as adult material, filtering products will still locate the page and filter it according to its content. Metadata is used to allow search engines to locate and recognize sites easily. Web site developers usually include metadata to increase the chances that search engines will include their site near the top of a list of search results. Because filtering companies use search engines to find potentially inappropriate sites, they are likely to find the large majority of sites with inappropriate images that users might actually see. (Testimony of Lorrie Cranor.)

154. Many filters combine and layer several of these different filtering techniques in order to increase the effectiveness and accuracy of their products. For example, Looksmart's product, NetNanny, and AOL's mature teen filter make use of black lists, white lists, and dynamic, real-time filtering. By combining these different approaches, filtering products have become increasingly effective. (Testimony of Lorrie Cranor; Whittle Dep. Tr. at 11:1-11:15; Murphy Dep. Tr. at 79:22-82:14.)

(iii) Non-content Filtering Aspects of Filtering Products

155. In addition to their content filtering features, filtering products have a number of additional tools to help parents control their children's Internet activities. Other tools available to parents include monitoring and reporting features that allow supervising adults to know which sites a minor has visited and what other types of activities a minor has engaged in online. AOL, for example, offers a feature called AOL Guardian, which provides a parent with a report indicating which Web sites a child visited, which sites were blocked, the number of emails and instant messages a child sent, and to whom a child sent email or instant messages. Surfcontrol similarly provides parents with reports of the sites a child has visited, as well as those that were blocked; their product also has the ability simply to monitor a child's activity without actually blocking anything, if a parent prefers that option. Contentwatch has a feature that permits parents to monitor their child's Internet activities remotely, for example, while they are at work. (Testimony of Lorrie Cranor; P. Exh. 5, 86; Whittle Dep. Tr. at 25:13-29:6; Murphy Dep. Tr. at 64:8-69:4.)

156. Several filtering products also provide parents with the option of having a warning appear before a child's access to certain material is permitted, rather than having the material blocked. The child will then have the option of going into the site, if he or she believes it is appropriate to view, or not going into the site, if it is deemed to be inappropriate or undesired. (Testimony of Lorrie Cranor.)

157. Many filtering programs also offer parents the ability to restrict the times of day that a child can use the Internet, or to control the total amount of time in a given day that a child may use it. Filtering software can similarly restrict Internet access by days of the week, making it possible for parents to make sure that their children only

access the Internet when an adult is home to supervise. (Testimony of Lorrie Cranor; P. Exh. 86; Whittle Dep. Tr. at 25:13-29:6; Murphy Dep. Tr. at 64:8-69:4.)

158. Filtering programs can also be used by parents to prevent their children from having any access to parts of the Internet other than the Web, and to certain Internet applications which parents do not want their children to have any access to, such as e-mail, chat, instant messaging, newsgroups, message boards and peer-to-peer file sharing. Some products also provide parents with the option of providing limited access to these Internet applications. For example, instant messaging and e-mail may be permitted, but some of the products will only permit the sending and receiving of messages from certain authorized individuals, and will block e-mails or instant messages containing inappropriate words. Filtering programs can also completely prevent children from entering or using chat rooms, or they can merely filter out any inappropriate words that come up during a chat session. Many of the products can also be set up to prevent children from inadvertently or intentionally sending out personal information, such as a home address or telephone number, and to block children from receiving downloads, attachments, or file transfers through any means. (Testimony of Lorrie Cranor; P. Exh. 6, 8, 54, 86, 88; Allan Dep. Tr. at 140:18-140:25; 141:1-142:25; 160:22-161:22; 163:4-164:23; Whittle Dep. Tr. at 16:18-24:22; 25:1-25:1; 30:14-31:5; 48:9-49:11; Murphy Dep. Tr. at 73:11-77:3, 110:13-113:25.)

(iv) Filters Are Widely Available

159. Filters are widely available and easy to obtain. Besides the numerous filtering products sold directly to consumers, filters are also available through ISPs. Eight of the top ten most used ISPs offer content filtering for free; the other two ISPs

(Verizon and United Online) offer it for rates of just $4.95 and $1.95 per month respectively. (Testimony of Lorrie Cranor; P. Exh. 86, 87, 88.)

160. Information comparing the relative quality, price and differing features of the internet content filtering products available for sale is readily available to consumers, for free, on the Internet. (P. Exh. 88.)

161. Estimates of the major ISP's market shares are:

ISP	Subscribers (in millions)	Market Share
1) America Online	18.6	20.1%
2) Comcast	9.0	9.7%
3) SBC (AT&T)	7.4	8.0%
4) Verizon	5.7	6.2%
5) Road Runner	5.4	5.8%
6) Earthlink	5.3	5.8%
7) BellSouth	3.1	3.4%
8) Cox	3.1	3.3%
9) United Online	2.8	3.0%
10) Charter	2.3	2.5%

162. Filters will also soon be pre-installed in computers using Microsoft's new operating system. Microsoft has announced plans to launch a new operating system called Vista by January 2007, which will contain Internet content filters, along with other access control tools for parents like time management, activity logging, and the ability to block or restrict children's access to online games. Anyone using this new operating system will automatically have access to these filtering tools. Vista will be compatible with third-party content filters, meaning that other companies will be able to classify content and provide those classifications in a format that will be readable by the Vista parental controls, enabling parents to configure third-party filters through the Vista control panel. Because the vast majority of computers come pre-loaded with Microsoft's

current operating system, Windows, the vast majority of computers will have built-in, free, compatible filters. (Testimony of Lorrie Cranor; P. Exh. 89.)

163. Microsoft has also announced that for those computers not using the new operating system, it will soon make a free content filter available as part of their Windows Live offering. Once the Windows Live parental controls are released, anyone with a computer running Windows XP will be able to download and use free parental controls software to filter content accessed with any Web browser. (Testimony of Lorrie Cranor.)

(v) Internet Content Filters are Easy to Use

164. Filtering programs are easy to install, configure, and use. (Testimony of Lorrie Cranor, Edward Felten; P. Exh. 3, 5, 6, 7, 8, 54, 84, 85, 86, 88.)

165. Almost all parents will be able to install filtering products and use them by selecting from one of their standard settings. Many filters, such as AOL Parental Controls and Cybersitter 9.0, have user interfaces that are quite easy to use and make it easy for users to create customized settings. (Testimony of Lorrie Cranor; P. Exh. P. Exh. 3, 5, 6, 7, 8, 54, 84, 85, 86, 88; Whittle Dep. Tr. at 7:9-8:4; 16:18-24:22; 25:1-25:1; 25:13-29:6; 41:19-42:1; Murphy Dep. Tr. at 79:22-82:14.)

166. Installation and initial configuration are areas that always pose some challenges for software users, and it is quite difficult to design software that absolutely everyone will find easy to use. Filtering software is no more difficult to install or use than other software that is widely used every day. For example, programs like Microsoft Word offer many options and settings that users have to navigate in order to use them effectively, and millions of people use such software. (Testimony of Lorrie Cranor, Edward Felten.)

167. Although there were occasional user complaints about latency (delay) with early-version filtering products, latency is much less of an issue with today's filtering products. Existing filters do not usually cause any significant or noticeable delays. The amount of time it typically takes filters to look URLs up in black lists and white lists is generally imperceptible. Even real-time filtering should take only slightly longer than the amount of time it normally takes to load a Web page – i.e., milliseconds. That is in part because the products have improved and eliminated most of those issues, and also because more and more Internet users are moving to higher speed broadband connections. (Testimony of Lorrie Cranor; Allan Dep. Tr. at 89:18-92:12; 170:13-171:14; Whittle Dep. Tr. at 99:21-101:4; 212:11-212:18.)

168. Installation problems and other technical issues, like compatibility, are disappearing as more and more people use filtering that is bundled with their ISP service or provided on the network rather than on each individual personal computer. In addition, many filtering products are now bundled together with other software, such as a larger security suite. As a result of these developments, customers no longer need to install stand-alone programs on their personal computers, and bundled filters are by definition compatible with a user's Internet service, along with any other security services offered through that provider. Windows Live and Windows Vista will similarly ease technical problems, because they will contain filters that, as part of the operating systems themselves, will work with any other program that is designed to be compatible with Windows. (Testimony of Lorrie Cranor; Murphy Dep. Tr. at 112:22-113:25)

(vi) Filters Cover More Speech than COPA

169. Even if COPA had been drafted differently to cover overseas Web sites, COPA cannot be enforced against a speaker who is not subject to U.S. law either because

he or she is outside the jurisdiction or for any other reason. (Testimony of Lorrie Cranor, Michael Russo; P.Exh. 6, 54.)

170. Filtering products can be used by parents to block speech on the Web no matter where the Web sites are located. (Testimony of Lorrie Cranor; P. Exh. 6, 54; Allan Dep. Tr. at 19:4-19:9; Whittle Dep. Tr. at 15:2-16:17; Murphy Dep. Tr. at 84:5-85:11, 88:10-88:19, 88:20-90:3, 91:20-92:9; Murphy Dep. Exh. 6, 7.)

171. Filtering products can be used by parents to block both non-commercial and commercial Web sites. (Testimony of Lorrie Cranor; P. Exh. 6, 54; Whittle Dep. Tr. at 157:6-159:16; Murphy Dep. Tr. at 84:5-85:11.)

172. Filtering products can be used by parents to block harmful to minors material that is paid for or free. (Testimony of Lorrie Cranor; Whittle Dep. Tr. at 157:6-159:16.)

173. Filtering products can be used by parents to block material that is distributed on the Web and on the other widely used parts of the Internet through protocols other than http. Specifically, filters can be used to block, among other things, e-mail, chat, instant messaging, peer-to-peer file sharing, newsgroups, streaming video and audio, Internet television and voice-over Internet telephone service. (Testimony of Lorrie Cranor; P. Exh. 6, 8, 54, 86, 88; Allan Dep. Tr. at 140:18-140:25; 141:1-142:25; 157:6-159:19; 160:22-161:22; 163:4-164:23; Whittle Dep. Tr. at 15:2-16:17; 16:18-24:22; 25:1-25:1; 30:14-31:5; 48:9-49:11; Murphy Dep. Tr. at 48:22-49:4, 49:13-50:11; Murphy Dep. Exh. 2.)

174. Filtering products will also better protect children and make the Internet a safer place for children than COPA because they reach a far broader range of content

than COPA, enabling parents to restrict their children's access to whatever kinds of content they choose, not just sexually explicit materials. For example, many products include categories like Violence, Drugs, Alcohol and Tobacco, Weapons and Criminal Skills. (Testimony of Lorrie Cranor; P. Exh. 5, 6, 7, 8, 54; Allan Dep. Tr. at 98:8-101:15; Whittle Dep. Tr. at 15:2-16:17; Murphy Dep. Tr. at 47:22-48:21, Murphy Dep. Exh. 2, 3.)

175. Filtering products also provide a more flexible solution than COPA because filtering products can be tailored to meet the individual values, desires, and needs of Internet users and/or their parents, and the age and maturity of a child. The wide range of user-based filtering options that are available at low or no cost permits parents and families to choose those options which are most consistent with their own family values and the circumstances of their children, including the age and maturity of each child, not the values of some other family or community. (Testimony of Lorrie Cranor; P. Exh. 5, 6, 7, 8, 54, 84, 85, 86, 88; Allan Dep. Tr. at 65:24-66:16; 68:7-70:13; Whittle Dep. Tr. at 7:9-8:4; 16:18-24:22; 25:1-25:1.)

176. Filtering products offer complete flexibility in that parents can turn them off any time they do not want to block material for themselves, other adults, or for their children. As a result, the potential for overblocking problems is greatly lessened in the context of voluntary parent-initiated filtering. (Testimony of Lorrie Cranor; P. Exh. 86; Allan Dep. Tr. at 16:18-24:22.)

(vii) Effectiveness of Filtering Products

177. Filtering products can be an effective tool to prevent children from accessing material deemed inappropriate for them, especially pornographic material. Although they are not perfect, filtering products block the vast majority of the material on

the Web that is sexually explicit and that might be considered harmful to minors. (Testimony of Lorrie Cranor, Terri Kirk, Clover Taylor, Tava Smathers; P. Exh. 3, 4, 5, 6, 7, 8, 11, 54, 85, 86, 88; Allan Dep. Tr. at 174:7-178:15; Whittle Dep. Tr. at 41:19-42:1.)

178. Individual filtering products vary in how effective they are at both accurately blocking intended material and not inadvertently blocking appropriate material. The better products are very good at blocking intended material and have very low rates of erroneously blocking material. (Testimony of Lorrie Cranor; P. Exh. 85, 86; Allan Dep. Tr. at 174:7-178:15; Whittle Dep. Tr. at 41:19-42:1.)

179. Filters can be made more restrictive or less restrictive and, thus, can block more or less material, depending on the individual desires of parents. The more willing a parent is to have some material inadvertently blocked, the more effective the product will be at blocking virtually all sexually explicit material. If a parent wants to make sure that his or her child does not have access to absolutely any sexually explicit material, the parent can set the filtering product accordingly and, in doing so, can make sure that there is an extremely low chance – likely less than 1% -- that such material will be accessible. (Testimony of Lorrie Cranor; P. Exh. 3, 4, 5, 6, 7, 8, 11, 54, 88; Allan Dep. Tr. at 181:23-184:25; Murphy Dep. Tr. at 46:8-47:17.)

180. Filters work especially well at blocking the most popular Web sites and the Web sites that are most likely to be accessed by a minor. For example, it is highly likely that every Web site that comes up in the first 50 results of a search engine query for "hard core porn" will be blocked by filtering products. Looksmart, for example, blocks

the first 50 results for Google and Yahoo searches for "hard core porn." (Testimony of Lorrie Cranor.)

181. The emergence and widespread popularity of search engines, which have led most Internet users to go to sites through described search engine links rather than typing a URL, combined with the Misleading Domain Name statute, has made it much less likely that a child will inadvertently access sexually explicit material if a filter is not being used, and even less likely if a filter is being used. (Testimony of Lorrie Cranor, Edward Felten.)

182. Many search engines, including Google, provide a filtering feature for parents to use to block results that contain material not appropriate for children. (Testimony of Lorrie Cranor.)

183. Many studies have been done to measure the effectiveness of various Internet content filtering products. The exact results of these studies often differ because of differences in their evaluation criteria and methodology. Evaluations of filter effectiveness usually focus on how accurate filters are at distinguishing between content that should and should not be blocked. "Under blocking" occurs when a filter fails to block content that is supposed to be blocked. "Over blocking" occurs when a filter blocks content that is not supposed to be blocked. (Testimony of Lorrie Cranor; Allan Dep. Tr. at 181:23-184:25.)

184. Although test results vary, most reports indicate that the better filters have under block rates of less than 10 percent, with some reporting underblock rates of less than 1 percent or in the 1-2 percent range. These filters typically have over block rates

that are lower than their under block rates when configured with settings designed for older children. (Testimony of Lorrie Cranor; P. Exh. 3, 4, 5, 7, 8, 88.)

185. Exact percentages will vary depending on the study's methodology and the Web sites tested. As expected, studies show that many filtering products are very accurate in connection with the most widely viewed or accessed sources of sexually explicit material. For that material, most products will have an underblock rate of less than 5 percent, and an even smaller overblock rate. Simply testing for random Web sites, that may never have been viewed by anyone in the United States, let alone minors, may lead to slightly higher underblock or overblock rates, but generally, several products will still have underblock rates of less than 10 percent. (Testimony of Lorrie Cranor; P. Exh. 3, 4, 5, 7, 8, 88.)

186. Studies have also shown that while filtering products block the vast majority of all material potentially inappropriate for children, the products are even better at blocking material that is clearly pornography and erotica, and they will block virtually all such material. (Testimony of Lorrie Cranor; P. Exh. 3, 4, 5.)

187. Two separate reports commissioned by Congress – from the Commission on Child Online Protection and the National Research Council – have confirmed that content filters can be effective at preventing minors from accessing harmful materials online. The COPA Commission report notes that filters can be effective in directly blocking global content, as well as content in newsgroups, email, and chat rooms. It points out that content filters are "flexible" and can be customized based on family choice. It also notes the existence and value of time management and logging features, particularly for encouraging parental involvement and influencing children's activities

online. Overall, it points out that "voluntary approaches provide powerful technologies for families." (Testimony of Lorrie Cranor; P. Exh. 6, 54.)

188. The National Research Council Report concurs, stating that "for parents who want to restrict access to the Internet, filters can be highly effective in reducing the exposure of minors to inappropriate content," and "it is helpful to regard such filtering as 'training wheels' for children on the Internet as they learn to make good decisions about what materials are and are not appropriate for their consumption." (Testimony of Lorrie Cranor; P. Exh. 54.)

189. Filtering products have improved over time and are now more effective than ever before, both in blocking intended material and in not blocking unintended material. (Testimony of Lorrie Cranor; P. Exh. 7, 8, 88; Murphy Dep. Tr. at 79:22-82:14.)

190. Filtering products today cover more speech than ever before, in more languages, and offer more options to parents to customize the products to fit the individual circumstances of their families and children. (Testimony of Lorrie Cranor; P. Exh. 7, 8, 88; Allan Dep. Tr. at 68:7-70:13; 73:4-73:6; Whittle Dep. Tr. at 7:9-8:4; 16:18-24:22; 25:1-25:1; 43:3-43:13; Murphy Dep. Tr. at 79:22-82:14.)

191. A major development for filtering products is that many products now provide multiple layers of filtering. Whereas filters once only relied on blacklists or whitelists, many of today's products utilize blacklists, whitelists, and real-time, dynamic filtering to catch any inappropriate sites that have not previously been classified by the product. This multi-layered approach has increased the effectiveness of content filters

and enables parents to block much more material if that is desired. (Testimony of Lorrie Cranor; Whittle Dep. Tr. at 11:1-11:15.)

192. There is a high level of competition in the field of Internet content filtering. That factor, along with the development of new technologies, has caused the products to improve over time. Given that consumer demand has not diminished, it is likely that the products will continue to improve and become even more effective over time. (Testimony of Lorrie Cranor; P. Exh. 8, 88; Murphy Dep. Tr. at 83:6-83:13, 142:10-142:18.)

193. Parents using filters are satisfied with their filtering products, and many believe the products are outperforming their expectations. For example, a study done for AOL found that 85 percent of parents are satisfied with their AOL Parental Controls products, and that 87 percent find them easy to use. (Testimony of Lorrie Cranor; P. Exh. 10, 84, 85; Murphy Dep. Tr. at 79:22-82:14.)

194. Many government agencies use Internet content filters on their computers. Testimony from the Department of Justice itself confirms that filtering products are effective at blocking sexually explicit material, that underblocking and overblocking are rarely reported as problems, and that Internet users are very satisfied with the way they work. (Joint stipulation at 90, 91, 92; Murphy Dep. Tr. at 95:16-96:13.)

195. Libraries also widely employ Internet filters. Despite personal views that full access to information is preferable, many librarians are very satisfied with the products and the way they work. As one example, in a 2003 article, Hampton Auld, a Virginia librarian, noted that during the first seventeen months of filtering in his library system, 2.4 million patrons surfed the Web and there were a mere 38 requests to unblock

and 38 requests to block Web sites. (Testimony of Terri Kirk, Clover Taylor, Tava Smathers; P. Exh. 9.)

196. Schools similarly use filters to make sure that their students do not encounter inappropriate material. Students are regularly testing the effectiveness of filters in real-world setting, by accessing thousands of Web sites per week from their school or school library computers. Many schools are satisfied with the protection and services offered by content filters. (Testimony of Larrie Cranor, Terri Kirk, Clover Taylor, Tava Smathers; P. Exh. 11.)

197. One of the features of filtering programs that adds to their effectiveness is that they have built-in mechanisms to prevent children from circumventing them, including password protection and devices to prevent children from uninstalling the product or adjusting a computer's clock to outsmart time settings. Some products have a tamper detection feature, by which they can detect when someone is trying to uninstall or disable the product, and then cut off Internet access altogether until it has been properly reconfigured. (Testimony of Lorrie Cranor, Edward Felten; Murphy Dep. Tr. at 71:16-72:20.)

198. Very few minors have the technical ability and expertise necessary to circumvent filtering products either by disabling the product on the actual computer or by accessing the Web through a proxy or intermediary computer to avoid a filter on the minor's computer. (Testimony of Lorrie Cranor, Edward Felten; P. Exh. 86; Whittle Dep. Tr. at 31:15-32:4; Murphy Dep. Tr. at 71:16-72:20; Allan Dep. Tr. at 148:22-150:11.)

199. Accessing the Web through a proxy or intermediary computer will not enable a minor to avoid a filtering product that analyzes the content of the Web page requested, in addition to where the page is coming from. Any product that contains a real-time, dynamic filtering component cannot be avoided by use of a proxy, whether the filter is located on the network or on the user's computer. (Testimony of Edward Felten.)

200. Filtering product companies actively search the Internet to identify any material that is posted online in an attempt to provide means to circumvent filtering products, and take steps to ensure that such material is blocked in the first place and cannot be used to circumvent their products. (Testimony of Lorrie Cranor, Edward Felten.)

201. The popularity of laptop computers is of no consequence to filtering products because they work on both desktop and laptop computers. Thus, if filtering software is installed on a laptop computer, it can filter Internet content wherever the computer is used, even if a child takes it outside the home. (Testimony of Lorrie Cranor; Murphy Dep. Tr. at 64:8-69:4.)

202. Filtering products are also designed to work if a family has more than one computer, as they can be installed on multiple computers in a home. (Testimony of Lorrie Cranor.)

(vii) Filtering Products Are Widely Used By Parents

203. Many people are using the parental control tools offered by content filtering products. Although the exact number of people using filters is difficult to determine, the most recent and most reliable studies have consistently found that about 55 percent of parents with Internet access at home are using filters. That figure shows that there has been a significant increase in filter use by parents – about a 65 percent increase

– from earlier studies conducted as recently as 2000. (Testimony of Lorrie Cranor, Andrew Gelman; P. Exh. 10, 35, 36.)

204. It is not known why some families do not use filters. Some parents may have decided that they are unnecessary or not desired (because they trust their children or for some other reason), some may be unaware of filters, or others may not use them for other reasons such as cost or (real or perceived) difficulty of use. (Testimony of Lorrie Cranor; P. Exh. 10, 84, 86; Whittle Dep. Tr. at 45:15-46:4.)

205. Filtering products are essentially one type of security software for use by computer owners. Statistics show that other highly effective security software products, such as anti-virus software, are not used by all computer owners for a variety of similar reasons. The percentage of users utilizing filtering products is not unexpected and is in fact a higher percentage of use than many analysts would have expected. (Testimony of Lorrie Cranor.)

206. Filtering products are widely used in most schools and libraries. Any school or library that receives federal funding for providing Internet access is required by a separate federal law, 21 U.S.C. § 9134; 47 U.S.C. § 254(h), to have filters installed and operating on all computers that are accessible by minors. (Testimony of Terri Kirk, Clover Taylor, Tava Smathers; Murphy Dep. Tr. at 93:19-94:10.)

(viii) Internet Content Filters For Use On New Technologies

207. Content from the Internet is now capable of being viewed on devices other than traditional personal computers. Examples include mobile devices such as mobile phones, personal digital assistants ("PDAs") such as the Blackberry, portable audio/video players such as the iPod, and game consoles. Many of these devices are essentially computers, packaged differently, and with differing user interfaces. (Testimony of

Edward Felten, Joseph Fried, Jonjie Sena; P. Exh. 20, 58-63; Murphy Dep. Tr. at 49:13-50:11.)

208. Although many devices are now capable of accessing the Internet, a very small percentage of individuals with such devices are actually using them to access the Internet. The percentage is even lower for the number of minors accessing the Internet through these devices. For those individuals who are using new devices to access the Internet, by far the most common use is to access email; because of both speed and cost issues, a significantly lower percentage of people use alternative devices to browse the Web. (Testimony of Joseph Fried, Jonjie Sena; Murphy Dep. Tr. at 96:17-97:19; Cingular Dep. Tr. at 39:24-40:20.)

209. Content filtering technology can be used on these alternative, non-PC devices, and there are no fundamental barriers to the feasibility of content filtering on the devices. It is possible to provide the same type and quality of content filtering for such devices as for ordinary computers. (Pl. Exh. 20, 58-63, 70; Allan Dep. Tr. at 166:4-167:18.)

210. Some alternative devices, such as certain PDAs and portable music players like the iPod, cannot receive content directly over the Internet, but can only receive it via a wired connection to a personal computer, after the content has been downloaded to the personal computer first. For these devices, the content will already have been subjected to the personal computer's Internet content filter, if the user has chosen to use a filtering product, so an additional filtering product for these devices is not necessary. (Testimony of Edward Felten.)

211. Filtering technology can be implemented for users of other alternative devices in several ways. One approach is to perform content filtering in the network, not on the device itself, much as is done for most ISP-based filters for personal computers. In this approach, equipment run by the network provider (e.g., the cellular network for a mobile phone) would observe, inspect, and filter network traffic in transit between the alternative device and the rest of the Internet. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena.)

212. Another approach is to run filtering software on the device itself. Devices such as mobile phones are really just small computers, which are capable of running the same types of software applications that desktop computers can run. The creator of a filtering program for desktop computers can simply take that program and modify it slightly so that it works on an alternative device. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena.)

213. Some alternative devices have less memory or slower processors than desktop computers. Less capable devices may have difficulty running some application programs. Due to the rapid and fairly predictable improvements in the capacity of memories and discs and the speed of processors, this state of affairs will only be temporary, and it is very likely that in the near future, almost all alternative devices will be able to run almost all applications that are used on personal computers today, including anti-virus software and content filtering software. (Testimony of Edward Felten.)

214. Yet another approach to implementing filtering for alternative devices is to pass the Internet content through a filter computer before delivering it to the end user's

device, using what is called an HTTP proxy. Standard Web browsers support an option to use an HTTP proxy. When a proxy is in use, and the browser needs to retrieve a file via HTTP, the browser does not request the file directly from the server that is offering it. Instead, the browser contacts the proxy and tells the proxy the URL of the file the browser wants. The proxy then contacts the server, retrieves the designated file, and passes the file back to the browser. Because the proxy handles every file (i.e., every page, image, etc.) that the browser gets, the proxy can filter the files to remove specified material, such as harmful to minors material. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena.)

215. Accessing the Web via a proxy, rather than accessing servers directly, makes no material difference in the amount of memory, computational power, or other resources that a mobile device will use. There is no noticeable difference for the user. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena.)

216. Mobile devices can, and often do, use HTTP proxies. The filtering proxy can be a computer (or bank of computers) anywhere on the Internet – it might be provided by a mobile phone company, by a filtering company, or by anyone else. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena.)

217. All of these filtering methods for alternative Internet access devices can be implemented transparently to the user, so the user's experience of using the device would be the same as it would be if the filter were not present (except for the unavailability of filtered content). The user interface for enabling, disabling, and controlling the filter could be essentially the same as on an ordinary computer. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena; Pl. Exh. 70.)

218. Several vendors, including large, experienced software companies, currently offer content filtering products for alternative devices. Examples include products offered by Ace*comm, Flash Networks, Bytemobile, Blue Coat, BCGI, Cisco, PureSight, Syniverse and RuleSpace, to name a few. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena; P. Exh. 58-64, 70.)

219. The companies that provide filtering products for traditional computers could also relatively easily modify their products for use on alternative devices. Many do not currently have products available for use on alternative devices because, given the recent emergence of such devices, there has not yet been a market demand for such products. Several of these companies are now considering whether to provide such a product, and once the demand is there, they are likely to provide such a filtering product. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena; Allan Dep. Tr. at 166:4-167:18.)

220. Several major mobile phone carriers, including Cingular, Sprint-Nextel, and Alltel, are offering parental controls features, including some content filtering, to enable parents to control their children's access to the Internet. These tools enable parents so desiring to, among other things, limit the Web content accessible through the phones to pre-selected, child friendly material, and prevent their children from using chat rooms, instant messaging, text messaging, email, purchasing any file downloads or having any access to the Internet at all. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena, Cingular Dep. Tr. at 7:4-7:23; 9:7-10:7; 11:12-12:10; 23:6-23:18; 24:12-26:4.)

221. Flash Networks has entered into an agreement with a major U.S. mobile carrier to enable the carrier to provide Flash Networks' content filtering product to its customers. Blue Coat's content filtering product is being used by the mobile operator Vodafone for its customers. Byetemobile's filtering product is being used by T-Mobile UK. Once the demand for content filtering on alternative devices emerges, it is highly likely that even more mobile carriers will provide such products. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena; P. Exh. 60.)

222. Ace*Comm's Parent Patrol product allows parents to impose usage restrictions on their children's cell phones, including restrictions based on time-of-day, service, specific phone numbers, and total talk time. Parent Patrol also includes content filtering. Ace*Comm has a contract with a North American carrier for deployment of elements of its Parent Patrol Product. (Testimony of Edward Felten, Jonjie Sena; P. Exh. 70.)

223. The major U.S. mobile carriers have agreed to abide by industry guidelines concerning Internet access and wireless content. Those guidelines require the carriers, among other things, to: (1) classify content into at least two categories – content available for all users and restricted content available for those over 18 years-old or those whose parents have specifically authorized access; (2) not provide access to restricted content until the carrier has deployed controls to restrict access to such material; (3) provide controls to restrict access to restricted content; and (4) consistent with each company's business plans, provide users with access to content filters that can restrict all Internet content not previously classified by the carrier. (Testimony of Edward Felten, Joseph Fried, Jonjie Sena; Cingular Dep. Tr. at 57:3-60:7; Cingular Dep. at Exh. 3.)

224. Parents who are especially concerned about their children accessing inappropriate content through their cell phones can take advantage of a different technology: cell phones designed specifically for children. (Testimony of Edward Felten; P. Exh. 64.)

(b) Other Less Restrictive Alternatives

(i) Prosecute Existing Laws: Obscenity Prosecutions

225. Despite repeated requests from private citizens, politicians, interest groups and others, there have been very few prosecutions for obscenity over the past ten years. (P. Exh. 65-68.)

226. Much of the material that might be considered harmful to minors and prosecutable under COPA would also be considered obscene and is therefore already prosecutable under existing laws. (Plaintiffs' Contention Interrogatories and attachments thereto; Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006; Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006; Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006; Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24; Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.)

227. The government's interest in protecting children from harmful to minors material could be addressed through vigorous enforcement of other existing criminal statutes. (P. Exh. 6, 54, 55.)

(ii) Misleading Domain Name Prosecutions

228. The Misleading Domain Name Statute (18 U.S.C. § 2252B) is designed to prevent Web site owners from disguising pornographic Web sites in a way likely to cause uninterested persons to visit them.

229. More vigorous prosecution of this statute would decrease the frequency with which minors inadvertently encounter unwanted sexually explicit material on the Internet.

(a) Congress Could Enact A More Limited, More Narrowly Tailored Statute.

(i) The Statute Could Apply to Images Only.

230. COPA's prohibition on material that is harmful to minors applies to any "communication, picture, image, graphic image file, article, recording, writing, or other matter." 47 U.S.C. § 231(e)(6). COPA therefore applies to written material with no images, and to audio recordings and other materials with no images.

231. Congress could enact a statute that only applies to material containing harmful to minors images or pictures. Such a statute would be less restrictive than COPA. (P. Exh. 54.).

(ii) The Statute Could Impose Only Civil Penalties.

232. COPA imposes significant criminal penalties, including imprisonment, in addition to severe civil penalties for violation of the statute. 42 U.S.C. § 231(a)(1).

233. Congress could enact a statute that provides only for civil penalties, and does not subject Web sites to potential criminal liability. Such a statute would be less restrictive than COPA.

(iii) The Statute Could Require Labeling of Harmful to Minors Material

234. COPA imposes severe criminal and civil penalties for distributing material that is harmful to minors over the Web. Congress could enact a statute that permits the distribution of such material, but instead requires Web site operators to include a rating, label, or code on the Web site that makes clear that harmful to minors material is available on the Web site. Such a rating, label or code could be placed on the initial home page of the site or in the hidden text, the metadata, associated with the site. (P. Exh. 54.)

235. A proposal to enact exactly this sort of statute has been endorsed by the current administration and has been introduced in Congress. The Department of Justice has issued public statements backing such a proposal as a means of protecting children. (Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2006, H.R. 5749, 109th Cong. (2006); Project Safe Childhood Act, S. 3432, 109th Cong. (2006).)

236. Requiring Web sites to include a harmful to minors rating, label or code would make filtering products even more effective and accurate at blocking harmful to minors material. (Testimony of Lorrie Cranor; P. Exh. 54.)

(iv) The Statute Could Require Filtering Products to Contain a Harmful to Minors Category.

237. In a separate statutory provision not challenged here, Congress has required that ISPs and online service providers make information about parental control tools such as filtering products available to their customers. Congress could enact a statute that requires all companies or individuals distributing Internet content filtering products to include a harmful to minors category for parents to use to block material

covered by COPA, and Congress could provide specific, express guidance as to what sorts of materials should be included in that category. (P. Exh. 54.)

238. Such a statute would enable companies that provide filtering products to block exactly the speech COPA seeks to prohibit. (Testimony of Lorrie Cranor.)

(v) Government-Provided List of Harmful to Minors Web Sites.

239. Congress could enact a statute requiring the Department of Justice or another governmental entity to compile and maintain a list of Web sites that contain material that is harmful to minors. Alternatively, the Department of Justice could do so on its own initiative. (Murphy Dep. Tr. at 99:9-100:22.)

240. Such a statute (or action) would provide filtering product companies with the ability accurately to block absolutely all speech that the government believes is harmful to minors. It would also provide parents and other entities with information about the types of material that are on the Web in order to assist parents in determining what protections, if any, are necessary for their children depending on their individual values and circumstances. (Testimony of Lorrie Cranor.)

241. Filtering product companies could also be forced, by statute, to include a harmful to minor category in their products that contains all of the Web sites included on the government's list. The State of Utah recently passed a law requiring its Attorney General to compile an "adult content registry," a list of harmful to minors but non-obscene URLs. The law requires ISPs, at customer request, to block access to URLs on the adult content registry. (Testimony of Lorrie Cranor; H.B. 260, 2005 Gen Sess. of 56th Leg. (Utah 1999).)

242. The filtering product companies would accept a governmentally-created list of inappropriate sites; in fact, many have already testified that they would almost certainly comply with any request from a governmental entity to include specific sites on their lists. (Testimony of Lorrie Cranor.)

(vi) Education: Encourage and Fund Educational Efforts

243. Teaching children how to use the Internet safely is an effective method of ensuring their protection. (Testimony of Lorrie Cranor, Terri Kirk, Clover Taylor, Tava Smathers; P. Exh. 6, 11, 54.)

244. Congress could encourage additional educational efforts through pilot programs and funding. (P. Exh. 6, 54.)

(vii) Other Parental Measures

245. Non-content filtering tools offered by filtering companies as well other parental measures are very valuable and effective in helping parents control their children's Internet activities. (Testimony of Lorrie Cranor; P. Exh. 6, 11, 54).

246. Parents can utilize other measures to monitor and guide their children's use of the Internet. This can include placing the computer in a family room where its use can be observed, establishing rules for use of the computer, monitoring the child's time on the computer, and tracking the Web sites to which the child goes. (Testimony of Lorrie Cranor; P. Exh. 6, 11, 54, 87.)

(viii) Funding of Independent Rating Systems

247. Congress could fund an independent organization to rate Web sites and make such ratings available to parents for their use. (P. Exh. 54.)

248. Such a rating system would make filtering products even more effective and accurate at blocking materials that are harmful to minors. (P. Exh. 54.)

III. PLAINTIFFS' PROPOSED CONCLUSIONS OF LAW

1. COPA is unconstitutional because it deprives adults of speech to which they are constitutionally entitled. Reno v. ACLU, 521 U.S. 844 (1997); Butler v. Michigan, 352 U.S. 380 (1957).

2. COPA is unconstitutional because it is not narrowly tailored to a compelling governmental purpose. Reno v. ACLU, 521 U.S. 844 (1997); Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002); Ashcroft v. ACLU, 524 U.S. 656 (2004).

3. COPA is unconstitutionally vague. Reno v. ACLU, 521 U.S. 844 (1997).

4. COPA is unconstitutionally overbroad. Reno v. ACLU, 521 U.S. 844 (1997).

5. COPA violates the First Amendment rights of older minors. Reno v. ACLU, 521 U.S. 844 (1997).

6. COPA violates the right to receive speech anonymously. McIntyre v. Bd. of Elections Comm'n, 514 U.S. 334 (1995); Lamont v. Postmaster General, 381 U.S. 301, 307 (1965); Denver Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727, 754 (1996); ACLU v. Johnson, 4 F. Supp. 2d 1029, 1033 (D. N.M. 1998).

Respectfully submitted,

_____/s/_____
Christopher A. Hansen
Aden Fine
Benjamin Wizner
Catherine Crump
American Civil Liberties Union
125 Broad Street – 18th floor
New York, NY 10004
(212) 549-2693

_____/s/_____
Christopher Harris
Seth Friedman
Katharine Marshall
Jeroen van Kwawegen
Elan R. Dobbs
Latham & Watkins LLP
885 Third Avenue
New York, NY 10022
(212) 906.1800

For Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on October 9, 2006, I electronically filed Plaintiffs' Proposed Findings of Fact and Conclusions of Law with the Clerk of the Court using the ECF system, which will send notification of such filing to Raphael O. Gomez, Department of Justice.

____/s/_____
Jeroen van Kwawegen
Latham and Watkins
885 Third Avenue
New York, NY 10022

Counsel for Plaintiffs